Международный союз электросвязи

МСЭ-Т X.1546

(01/2014)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Обмен информацией, касающейся кибербезопасности – Обмен информацией о событии/инциденте/эвристических правилах

Перечень и характеристики атрибутов вредоносного программного обеспечения

Рекомендация МСЭ-Т X.1546

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

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

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

Рекомендация МСЭ-Т X.1546

Перечень и характеристики атрибутов вредоносного программного обеспечения

Резюме

Язык перечня и характеристик атрибутов вредоносного программного обеспечения (MAEC) включает перечни атрибутов и видов поведения вредоносного программного обеспечения, которые образуют общий словарь. Эти перечни относятся к разным уровням абстракции: "наблюдаемые" низкого уровня, виды поведения среднего уровня и таксономии высокого уровня. Рекомендация МСЭ-Т X.1546, которая является первоначальной версией MAEC, посвящена созданию списка низкоуровневых атрибутов вредоносного программного обеспечения. В ней максимально используются некоторые примеры аналогичной работы, проделанной в этой области. Таким образом, первоначально данная Рекомендация позволит описать характеристики наиболее распространенных типов вредоносного программного обеспечения, в том числе троянов, червей и руткитов, однако в перспективе она будет применима к гораздо менее распространенным типам вредоносного программного обеспечения.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный ID*
1.0	МСЭ-Т X.1546	24.01.2014 г.	17-я	11.1002/1000/12038

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Введение

Рекомендация МСЭ-Т X.1546, касающаяся использования перечня и характеристик атрибутов вредоносного программного обеспечения (MAEC), является коллективно разработанным международным стандартом по вопросам информационной безопасности, который содействует формированию открытого и общедоступного контента по тематике безопасности, касающегося вредоносного программного обеспечения и его поведения. Данная Рекомендация направлена на стандартизацию передачи этой информации по всему спектру средств и услуг обеспечения безопасности, которые могут использоваться для мониторинга и управления защитой от вредоносного программного обеспечения. MAEC – это язык, который используется для кодирования подробной информации, относящейся к вредоносному программному обеспечению.

Язык MAEC предназначен для: 1) совершенствования обмена информацией по вопросам вредоносного программного обеспечения, осуществляемого в направлении человек-человек, человек-средство, средство-средство и средство-человек; 2) уменьшения возможного дублирования работы по анализу вредоносного программного обеспечения, проводимой исследователями; и 3) создания условий для ускоренной разработки мер противодействия путем обеспечения возможности максимального использования мер реагирования на ранее наблюдавшиеся образцы вредоносного программного обеспечения. Анализ угроз, обнаружение вторжения и управление инцидентами – это процессы, которые касаются всех типов киберугроз. Благодаря единообразному кодированию атрибутов вредоносного программного обеспечения, язык MAEC предоставляет стандартный формат для включения в эти процессы информации, позволяющей принять меры, которая касается вредоносного программного обеспечения.

Вредоносное программное обеспечение (malicious software), называемое также "malware", существует в той или иной форме со времени появления первого компьютерного вируса в 1971 году. В настоящее время оно несет ответственность за множество вредоносных действий – от огромной доли спама в электронной почте, распространяемого с помощью бот-сетей, до кражи ценной информации посредством целевых атак методами социальной инженерии. Являясь, по сути, автономным агентом, действующим от имени злоумышленника, вредоносное программное обеспечение способно выполнять любое действие, которое может быть выражено в виде кода, и в связи с этим представляет огромную угрозу кибербезопасности.

Таким образом, защита компьютерных систем от вредоносного программного обеспечения является сегодня одной из наиболее важных задач информационной безопасности для организаций и частных лиц. Это связано с тем, что даже единственный образец пропущенного вредоносного программного обеспечения может привести к повреждению систем и раскрытию данных. Как показывает пример с вредоносным программным обеспечением, использующим USB-накопитель в качестве "инсерционного вектора", отсутствие соединения с компьютерной сетью не полностью устраняет риск заражения. По сути, до настоящего времени большинство усилий по противодействию вредоносному программному обеспечению было сосредоточено на предотвращении вредного воздействия посредством раннего обнаружения.

В настоящее время существует несколько распространенных методов, используемых для обнаружения вредоносного программного обеспечения, которые основаны, главным образом, на физических сигнатурах и эвристике. Эти методы эффективны с точки зрения их узкой направленности, хотя им присущи индивидуальные недостатки. Например, известно, что сигнатуры непригодны для противодействия вирусам "нулевого дня", целевым и полиморфным вирусам, а также другим видам появляющегося вредоносного программного обеспечения. Аналогичным образом, эвристическое обнаружение способно в общем обнаруживать определенные типы вредоносного программного обеспечения и при этом пропускать те из них, для которых отсутствуют шаблоны, например руткиты уровня ядра. Поэтому не будет ошибкой сказать, что при существующем потоке вредоносного программного обеспечения нельзя полагаться исключительно на эти методы, несмотря на то, что они по-прежнему являются полезными.

Перечень и характеристики атрибутов вредоносного программного обеспечения (MAEC, произносится, как "майк") предназначены для устранения неоднозначности и неточности, которая сегодня существует в описаниях вредоносного программного обеспечения, и сокращения использования сигнатур. Таким образом, язык MAEC направлен на совершенствование обмена информацией о вредоносном программном обеспечении, осуществляемого в направлении человек-человек, человек-средство, средство-средство и средство-человек; уменьшение возможного дублирования работы по анализу вредоносного программного обеспечения, проводимой исследователями, и создание условий для ускоренной разработки мер противодействия путем

обеспечения возможности максимального использования мер реагирования на ранее наблюдавшиеся образцы вредоносного программного обеспечения. Будет наглядно показано, что язык MAEC обеспечивает возможность корреляции, интеграции и автоматизации применительно к обмену структурированной информацией о вредоносном программном обеспечении на основе атрибутов, например видов поведения, артефактов и схем атак.

Как показано на рисунке 1, язык MAEC состоит из модели данных, которая охватывает несколько взаимосвязанных схем, представляющих таким образом грамматику, которая определяет язык. Эти схемы допускают создание различных форм выходных данных MAEC, которые могут считаться конкретными случаями использования указанной выше грамматики.

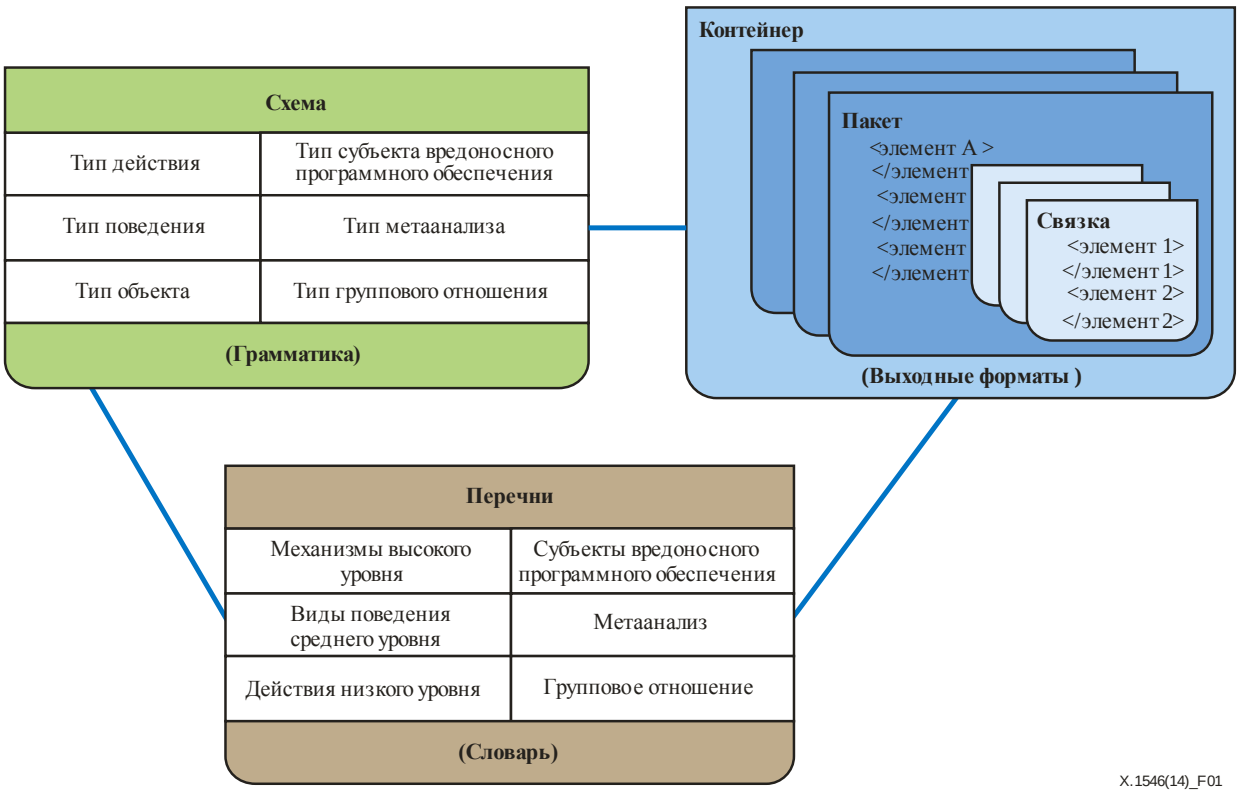

Рисунок 1 – Обзор высокого уровня MAEC

Схемы контейнера MAEC, пакета MAEC и связки MAEC предназначены для различных случаев использования и, соответственно, собирают разные типы информации, касающейся вредоносного программного обеспечения.

Язык MAEC связан с языком описания "кибернаблюдаемых" (CybOX) и с форматом обмена метаданными вредоносного программного обеспечения (MMDEF), разработанным ICSG IEEE.

CybOX – это стандартизированный язык описания, сбора, определения характеристик и обмена информацией о событиях или свойствах, отражающих состояние, которые наблюдаются в операционном домене. "Кибернаблюдаемые" имеют отношение ко многим доменам, в том числе оценке и характеристикам угроз (подробные схемы атак), характеристикам вредоносного программного обеспечения, управлению операционными событиями, регистрации событий, осведомленности о ситуации в киберпространстве, реагированию на инциденты, цифровому экспертно-техническому анализу и обмену информацией о киберугрозах.

Практически каждое поле в CybOX является необязательным, поэтому можно использовать любые нужные поля и пропустить остальные. Язык CybOX может использоваться для описания и определения характеристик целого ряда киберобъектов. Он может также использоваться для определения реляционных и логических структур нескольких объектов, действий, событий и/или "наблюдаемых".

При определении характеристик вредоносного программного обеспечения с помощью MAEC используется предоставляемый CybOX общий механизм (структура и контент) рассмотрения "кибернаблюдаемых" по всему перечню случаев использования MAEC. Язык MAEC предоставляет контекст, признаки, виды поведения и механизмы, необходимые для анализа, а CybOX приводит общие

действия и объекты, используемые в операционном кибердомене. "Кибернаблюдаемое" – *это измеряемое событие или отражающее состояние свойство* в кибердомене. Примеры измеряемых событий включают создание ключа системного реестра, удаление файла и прием запроса HTTP GET; примеры отражающих состояние свойств включают хэш-функцию MD5 какого-либо файла, значение ключа системного реестра и наличие взаимоисключений.

MAEC импортирует и расширяет объект и действие CybOX. Крайне упрощенный обзор схемы CybOX изображен на рисунке 2; компоненты CybOX, которые используются MAEC, показаны зеленым цветом.

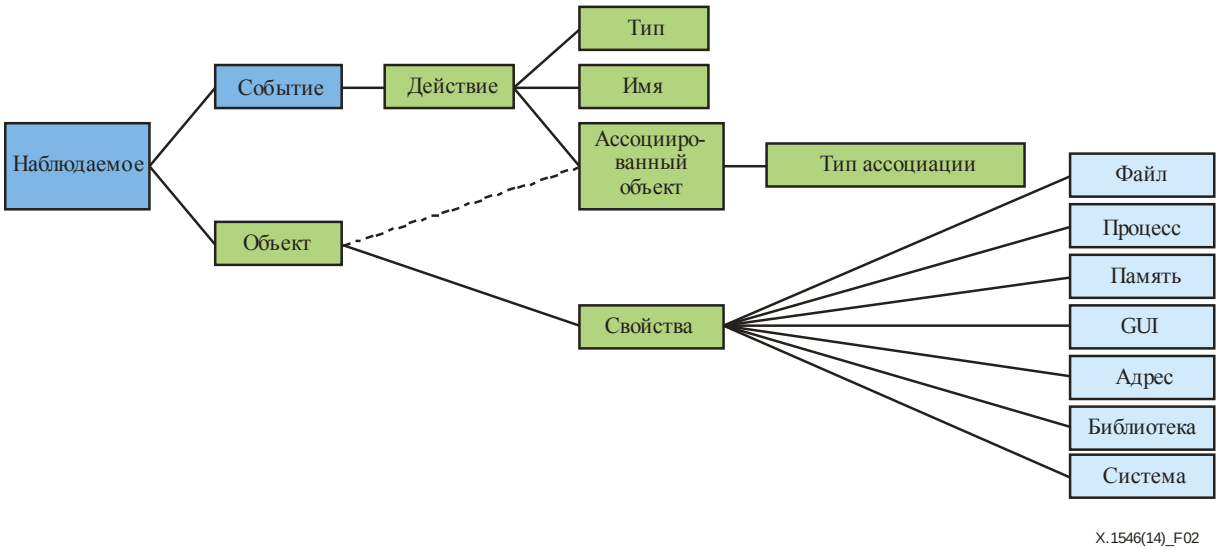

Рисунок 2 – Упрощенный обзор схемы описания "кибернаблюдаемых" (CybOX)

Структурный компонент свойств CybOX – это абстрактное поле для заполнения, предназначенное для различных заранее определенных схем типа объекта (например, файл, процесс, память), которые могут быть реализованы на его месте. Схемы свойств, показанных голубым цветом, обеспечиваются независимо от базовой схемы CybOX.

Разработка формата MMDEF осуществляется Отраслевой группой по безопасности соединений (ICSG) Института инженеров по электротехнике и радиоэлектронике (IEEE). Разработка первоначальной схемы осуществлялась главным образом группой поставщиков антивирусных (AV) продуктов с целью получения способа добавления дополнительных метаданных к образцам вредоносного программного обеспечения, которыми осуществлялся обмен. По сути, этот формат позволяет определять характеристики некоторых статичных свойств, например хэш-функций и имен файлов, а также ряд самых базовых характеристик поведения.

Сообщество информационной безопасности способствует разработке MAEC, участвуя в создании языка MAEC в рамках дискуссионных списков разработчиков MAEC и портала для совместной работы, а также путем включения языка MAEC в свои средства и возможности репозитория. В сообщество MAEC входят представители целого ряда отраслевых, академических и правительственных организаций из многих стран мира, которые осуществляют надзор и совместную деятельность в области языка MAEC, а также сервисных программ и средств MAEC через общедоступный репозиторий. Из этого следует, что в языке MAEC отражена ценная информация и объединенные специальные знания, полученные от максимально широкого круга специалистов всего мира в области анализа и предотвращения распространения вредоносного программного обеспечения.

Настоящая Рекомендация разработана в сотрудничестве с корпорацией MITRE с учетом важности обеспечения в максимально возможной степени технической совместимости между данной Рекомендацией и документом "Требования и Рекомендация в отношении совместимости с MAEC", версия 1.1 от 7 июля 2013 года.

[https://maec.mitre.org/compatible/Requirements_for_MAEC_Compatibility_V1.1.pdf].

Рекомендация МСЭ-Т X.1546

Перечень и характеристики атрибутов вредоносного программного обеспечения

1 Сфера применения

В настоящей Рекомендации представлены структурированные средства, содействующие формированию открытого и общедоступного контента по тематике безопасности, касающегося вредоносного программного обеспечения и его поведения, а также стандартизации передачи этой информации по всему спектру средств и услуг обеспечения безопасности, которые могут использоваться для мониторинга и управления защитой от вредоносного программного обеспечения.

2 Справочные документы

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

[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 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 владелец (owner) [b-ITU-T X.1520]: Хранитель (реальное физическое лицо или компания), несущий ответственность за данную возможность.

3.1.2 пользователь (user) [b-ITU-T X.1520]: Потребитель или потенциальный потребитель конкретной возможности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 возможность (capability): Конкретная функция или функции продукта, услуги или репозитория.

3.2.2 результаты теста возможности (capability test results): Данные об итогах тестирования на правильность.

3.2.3 контент (content): Любая форма объекта перечня и характеристик атрибутов вредоносного программного обеспечения (MAEC), в том числе документы в выходном формате MAEC, а также вложенные элементы/типы.

3.2.4 тестирование на правильность (correctness testing): Процесс определения того, правильно ли то или иное средство реализовало MAEC.

3.2.5 связка MAEC (MAEC bundle): Одна из стандартных форм выходных данных MAEC, предназначенная для сбора всех полученных в результате анализа характеристик одного образца вредоносного программного обеспечения, в том числе любых наблюдаемых видов поведения или действий MAEC, а также любых связанных с ним объектов MAEC.

3.2.6 контейнер MAEC (MAEC container): Одна из стандартных форм выходных данных MAEC, предназначенная для сбора одного или нескольких пакетов MAEC.

3.2.7 выходной формат MAEC (MAEC output format): Любая из трех стандартных форм выходных данных MAEC, включающая контейнер, пакет или связку MAEC.

3.2.8 пакет MAEC (MAEC package): Одна из стандартных форм выходных данных MAEC, предназначенная для описания всех известных данных для одного или нескольких субъектов вредоносного программного обеспечения, в том числе полученных в результате анализа характеристик (через связки MAEC) и любых соответствующих данных анализа или других метаданных.

3.2.9 образец вредоносного программного обеспечения (malware instance): Конкретная копия вредоносного программного обеспечения.

3.2.10 элемент вредоносного программного обеспечения (malware element): Поведение, атрибут, эксплойт, вредоносная нагрузка и т. д., относящееся к конкретному образцу и семейству вредоносного программного обеспечения или классу образцов вредоносного программного обеспечения.

3.2.11 шаблон вредоносного программного обеспечения (malware pattern): Абстракция некоторых атрибутов, присущих набору образцов вредоносного программного обеспечения (семействам или классам). Теоретически, один шаблон вредоносного программного обеспечения может иметь множество различающихся образцов вредоносного программного обеспечения, ассоциируемых с ним.

3.2.12 субъект вредоносного программного обеспечения (malware subject): Объект MAEC, который собирает всю подробную информацию, относящуюся к одному образцу вредоносного программного обеспечения, в том числе любые соответствующие метаданные для анализа, контент анализа и информацию об отношении.

3.2.13 продукт (product): Любое средство, услуга или репозиторий, предназначенное для противодействия вредоносному программному обеспечению, которое имеет одну или несколько возможностей.

3.2.14 репозиторий (repository): Явная или неявная совокупность элементов вредоносного программного обеспечения или шаблонов вредоносного программного обеспечения, которая поддерживает средство или услугу создания контента, например база данных шаблонов поведения, набор образцов вредоносного программного обеспечения, анализируемых средством экспериментальной среды, или суммарные выходные данные средства статичного или динамичного двоичного анализа. Репозиторий может также являться совокупностью документов в выходном формате MAEC.

3.2.15 рассмотрение (review): Процесс определения того, совместима ли та или иная возможность с MAEC.

3.2.16 орган по рассмотрению (review authority): Организация, осуществляющая тестирование на правильность и уполномоченная официально подтверждать, что та или иная возможность совместима с MAEC.

3.2.17 выборка для рассмотрения (review sample): Копия выходных данных возможности, предоставленная органу по рассмотрению для использования при определении того, совместима ли та или иная возможность с MAEC.

3.2.18 версия для рассмотрения (review version): Датированная версия MAEC, которая используется для определения совместимости возможности с MAEC.

3.2.19 услуга (service): Деятельность по анализу, обнаружению или устранению вредоносного программного обеспечения, которая реализует одну или несколько возможностей.

3.2.20 средство (tool): Программное приложение или устройство, которое реализует одну или несколько функций. Средство осуществляет анализ, обнаружение или устранение вредоносного программного обеспечения с помощью различных методов, например, существует средство статического анализа, средство динамического анализа, сигнатурный сканер, эвристический сканер и т. д. Средство может также осуществлять авторскую разработку контента.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

AV	Antivirus	Антивирус
CybOX	Cyber-Observable expression	Описание "кибернаблюдаемых"
ID	Identifier	Идентификатор
MAEC	Malware Attribute Enumeration and Characterization	Перечень и характеристики атрибутов вредоносного программного обеспечения
MMDEF	Malware Metadata Exchange Format	Формат обмена метаданными вредоносного программного обеспечения
SIM	Security Information Management	Управление информацией о безопасности
XML	Extensible Markup Language	Расширяемый язык разметки

5 Соглашения по терминологии

В настоящей Рекомендации сокращение MAEC используется как имя существительное.

6 Требования высокого уровня

Указанные ниже элементы определяют понятия, роли и ответственности, связанные с пятью различными возможностями, ориентированными на какое-либо отличное использование языка MAEC, которые составляют надлежащее использование языка MAEC. Эти возможности позволяют каждому члену сообщества MAEC легко понять, как данный продукт использует язык MAEC и как он может удовлетворить их потребности.

Указанные ниже требования относятся ко всем возможностям, осуществляющим поддержку MAEC, независимо от конкретной реализуемой функции (требования, специфичные для функций, приведены ниже, в пункте 10 "Конкретные требования к совместимости"). Если возможность удовлетворяет всем применимым требованиям, то владелец соответствующей возможности должен получить от органа по рассмотрению официальное подтверждение о совместимости с MAEC.

Необходимые условия

6.1 Владелец возможности должен являться действительным субъектом права, т. е. организацией или физическим лицом, имеющим действительный номер телефона, адрес электронной почты и почтовый адрес.

6.2 Владелец возможности должен согласиться соблюдать все обязательные требования к совместимости с MAEC, которые включают обязательные требования для данной конкретной функции.

6.3 Владелец возможности должен предоставить органу по рассмотрению техническое лицо для контактов, обладающее достаточной квалификацией, для того чтобы отвечать на вопросы о любой относящейся к MAEC функции, составляющей возможность, и координировать подготовку возможности для тестирования на правильность.

6.4 Владелец возможности должен предоставить органу по рассмотрению заполненную "Форму вопросника по совместимости с MAEC". Эта форма предоставляется владельцу возможности после обработки органом по рассмотрению "Формы декларации о совместимости с MAEC".

6.5 Владелец возможности должен сотрудничать с органом по рассмотрению и предоставить в его распоряжение соответствующий продукт, услугу или репозиторий в целях тестирования на правильность.

6.6 Владелец возможности должен предоставить органу по рассмотрению свободный доступ к элементам, необходимым для тестирования на правильность, в том числе к результатам теста и/или выборке для рассмотрения, для того чтобы определить их соответствие всем установленным требованиям к совместимости.

6.7 В качестве одного из условий получения официального подтверждения о совместимости с MAEC владелец возможности должен согласиться оказывать поддержку органу по рассмотрению в последующей деятельности по итогам тестирования, при которой производится обмен файлами соответствующих типов с другими организациями, стремящимися доказать правильность их возможности. Управление этим процессом осуществляется органом по рассмотрению, что потребует разумных усилий со стороны всех участвующих сторон.

6.8 Возможность должна быть доступна для населения или группы потребителей.

6.9 Возможность должна четко указывать версию(и) MAEC, использованную для рассмотрения, и соответствующую схему(ы), с которой она совместима.

Разное

Данные требования касаются разных аспектов совместимости с MAEC.

6.10 Если соответствующая возможность не удовлетворяет всем применимым требованиям, перечисленным выше (пп. 6.1–6.9), то владелец этой возможности не должен объявлять о ней, как о совместимой с MAEC.

6.11 Если соответствующая возможность не удовлетворяет требованиям, специфичным для ее функций (определенным ниже в пп. 10.1–10.27), то владелец этой возможности не должен объявлять о ней, как о совместимой с MAEC.

6.12 Прежде чем объявлять о возможности, как о совместимой с MAEC, ее владелец должен получить официальное утверждение от органа по рассмотрению.

7 Правильность

Данные требования касаются ошибок в определении правильности совместимости с MAEC, включая, в том числе ошибки, связанные со схемой валидации и недействительным использованием конкретных структур и элементов MAEC.

7.1 Владелец возможности должен располагать средствами, позволяющими пользователю представить ошибки правильности, выявленные им при использовании MAEC, а также в любом контенте MAEC, производимом этой возможностью.

7.2 Владелец возможности должен иметь действующий план по устранению любых ошибок правильности, о которых ему было сообщено.

7.3 Владелец возможности должен устранять любые ошибки правильности, о которых ему было сообщено, в пределах разумного периода времени после первого сообщения о данной ошибке.

8 Документация

К документации, которая представляется вместе с возможностью, совместимой с MAEC, применяются следующие требования.

8.1 Документация на возможность должна включать краткое описание MAEC и совместимости с MAEC, которое может включать дословно цитируемые части документов с веб-сайта MAEC.

8.2 В документации на возможность должна быть четко указана полнота охвата MAEC и соответствующих схем, включая схемы, полученные в результате коллективных усилий в области описания "кибернаблюдаемых" (CybOX) и формата обмена метаданными вредоносного программного обеспечения (MMDEF), либо посредством элементов или отдельных объектов CybOX, которые она не поддерживает, либо посредством элементов или объектов CybOX, которые она поддерживает. Например, если какая-либо возможность претендует на официальное подтверждение о совместимости с MAEC в качестве средства или услуги создания контента динамического анализа, и она не поддерживает объект файла CybOX и/или действия, связанные с объектом файла CybOX, то в документации на эту возможность должно быть прямо указано на данную несовместимость.

8.3 В документации на возможность должна быть четко указана процедура, которой должен придерживаться пользователь при представлении ошибок правильности, выявленных им в любом контенте MAEC, производимом продуктом.

8.4 Если документация, относящаяся к возможности, включает предметный указатель, то она должна включать ссылки на документацию, связанную с MAEC, под термином "MAEC".

9 Действительность

Указанные ниже требования вытекают из требования о том, что возможности, совместимые с MAEC, должны работать с действительными документами. Такие требования помогают обеспечить правильное форматирование информации и соответствие структуры документа языку MAEC.

9.1 Возможность должна валидировать весь контент MAEC (как произведенный, так и потребленный), используя валидацию на основе языка XML Schema консорциума W3C (см. [W3C XML Schema]), на его соответствие версии языка MAEC, которой, как было заявлено, она соответствует.

9.2 Возможность должна сообщать пользователю о любых ошибках валидации на основе языка XML Schema консорциума W3C.

9.3 Возможность должна валидировать весь контент MAEC (как произведенный, так и потребленный), используя валидацию на основе языка Schematron (см. [ISO/IEC 19757-3]) на его соответствие версии языка MAEC, которой, как было заявлено, она соответствует.

9.4 Возможность должна сообщать пользователю о любых ошибках валидации на основе языка Schematron.

10 Конкретные требования к возможностям

Указанные ниже требования относятся только к тем возможностям, применительно к которым владельцы возможностей добиваются совместимости с MAEC в отношении связанных с ними функций. Возможность, совместимая с MAEC, должна обеспечивать как минимум одну конкретную функцию: создание контента, хранение контента и потребление контента.

Создание контента	Средство или услуга, которое создает новые файлы MAEC или оказывает помощь в процессе их создания, включая те средства или услуги, которые объединяют существующие документы в выходном формате MAEC в один файл. Ниже определяются следующие подвиды функции создания контента: • Создание контента статического анализа: Средство или услуга, которое осуществляет некоторый статический анализ одного или нескольких образцов входного вредоносного программного обеспечения и выводит результаты в виде документа в выходном формате MAEC. • Создание контента динамического анализа: Средство или услуга, которое осуществляет некоторый динамический анализ (т. е. практическое выполнение) образца входного вредоносного программного обеспечения и выводит результаты в виде документа в выходном формате MAEC. • Создание авторского контента: Средство или услуга, которое поддерживает создание и редактирование документов в выходном формате MAEC вручную.
Хранение контента	Предоставление репозитория контента MAEC в распоряжение сообщества (бесплатно или на платной основе).
Потребление контента	Средство или услуга, которое принимает документы в выходном формате MAEC в качестве входных документов и либо отображает их содержимое пользователю, либо использует их для осуществления некоторого действия (устранения, управления информацией о безопасности (SIM) и т. д.).

Создание общего контента

Данные требования применяются ко всем средствам и услугам, которые предназначены для предоставления выходных данных контента MAEC.

10.1 Средство или услуга, которое предоставляет контент MAEC, должно создавать как минимум один тип выходного формата MAEC (связку, пакет или контейнер MAEC).

10.2 Каждое средство или услуга, предназначенное для предоставления выходных данных в отношении одного образца вредоносного программного обеспечения и не предназначенное для сбора информации о его собственных атрибутах, должно создавать одну связку MAEC для образца вредоносного программного обеспечения.

10.3 Средство или услуга, предназначенное для предоставления выходных данных в отношении одного образца вредоносного программного обеспечения, и/или предназначенное для сбора информации о его собственных атрибутах, должно создавать один или несколько пакетов MAEC с одним или несколькими вложенными субъектами вредоносного программного обеспечения MAEC для каждого образца вредоносного программного обеспечения, анализ которого оно проводит. Если средство или услуга не создает пакеты MAEC, то оно должно создавать контейнеры MAEC, которые содержат вложенные пакеты MAEC.

10.4 Средство или услуга, предназначенное для предоставления выходных данных в отношении более чем одного набора или группы образцов вредоносного программного обеспечения, должно создавать один или несколько контейнеров MAEC с одним или несколькими вложенными пакетами MAEC в отношении каждого набора или группы образцов вредоносного программного обеспечения, анализ которого оно проводит.

10.5 Средство или услуга, предназначенное для сбора информации о своих собственных атрибутах, должно указывать, как минимум, свое название, версию и производителя, используя соответствующие объекты в субъекте вредоносного программного обеспечения MAEC и в дальнейшем должно создавать пакеты MAEC или контейнеры с вложенными пакетами MAEC.

10.6 Средство или услуга, которое создает пакеты MAEC, должно иметь возможность создания отдельных связок MAEC.

10.7 Средство или услуга, которое создает контейнеры MAEC, должно иметь возможность создания отдельных пакетов MAEC.

10.8 Средство или услуга должно использовать собственную постоянную уникальную часть идентификатора (ID), отведенную под пространство имен, во всем создаваемом им контенте MAEC.

Создание контента статического анализа

Данные требования применяются ко всем средствам и услугам статического анализа, которые предназначены для создания контента MAEC.

10.9 При создании файла в выходном формате MAEC средство или услуга статического анализа должно сообщать о своих выводах, используя наиболее подходящие объекты MAEC (включая, в том числе, действия, объекты, виды поведения MAEC и/или классификации антивирусов), а также наиболее подходящий выходной формат MAEC.

Создание контента динамического анализа

Данные требования применяются ко всем средствам и услугам динамического анализа, которые предназначены для создания контента MAEC.

10.10 При создании файла в выходном формате MAEC средство или услуга динамического анализа должно сообщать о своих выводах, используя наиболее подходящие объекты MAEC (включая, в том числе, действия и виды поведения MAEC), а также наиболее подходящий выходной формат MAEC.

Создание авторского контента

Данные требования применяются ко всем средствам и услугам, предназначенным для создания контента MAEC или содействия в создании или изменении контента MAEC.

10.11 Средство или услуга авторской разработки должно стимулировать повторное использование существующих субъектов, видов поведения, действий, объектов и возможных признаков вредоносного программного обеспечения.

10.12 Средство или услуга авторской разработки должно обеспечивать пользователю возможность инициировать валидацию документа, написанного для языка MAEC, и сообщать ему обо всех ошибках, выявленных с использованием языка XML Schema консорциума W3C и языка Schematron.

10.13 Средство или услуга авторской разработки должно обеспечивать пользователю возможность импортировать и редактировать существующий контент MAEC (данная возможность включает все выходные форматы MAEC).

10.14 Средство или услуга авторской разработки должно обеспечивать пользователю возможность экспортировать контент, созданный в виде действительных документов в выходном формате MAEC.

10.15 Средство или услуга авторской разработки должно сообщать пользователю о дублированном контенте.

10.16 Средство или услуга авторской разработки должно обеспечивать ценность и возможности, превышающие возможности редактора расширяемого языка разметки (XML), как это определено органом по рассмотрению.

Хранение контента

Данные требования применяются ко всем репозиториям, которые предназначены для предоставления совокупности контента MAEC.

10.17 Каждый контейнер, пакет, субъект вредоносного программного обеспечения, результаты анализа, связка, действие, объект, поведение, возможный признак, совокупность видов поведения, совокупность действий, совокупность объектов и совокупность возможных признаков MAEC должен содержать уникальный ID по отношению ко всем остальным контейнерам, пакетам, субъектам вредоносного программного обеспечения, результатам анализа, связкам, действиям, объектам, видам поведения, возможным признакам, совокупностям видов поведения, совокупностям действий, совокупностям объектов и совокупностям возможных признаков MAEC в данном репозитории.

10.18 Каждое действие и объект MAEC должно содержать ID по отношению ко всем остальным действиям и объектам MAEC, при этом такой ID является уникальным по отношению ко всем остальным действиям и объектам MAEC в данном репозитории.

10.19 Часть ID, отведенная под пространство имен, должна быть постоянной во всем контенте MAEC и должна быть уникальной для данного репозитория.

10.20 Каждый контейнер, пакет, субъект вредоносного программного обеспечения, результаты анализа, связка, действие, объект, поведение, возможный признак, совокупность видов поведения, совокупность действий, совокупность объектов и совокупность возможных признаков MAEC должен иметь одинаковый ID на протяжении периода своего существования. Существующий элемент не должен заменяться в каких-либо иных целях, так как пользователи могут делать на него ссылку в собственном контенте.

10.21 Владелец репозитория должен прописать процесс, посредством которого пользователь может извлечь обновления контента.

Потребление контента

Данные требования применяются ко всем средствам и услугам, которые предназначены для потребления контента MAEC. Следует отметить различие между термином "потреблять" (осуществлять интеллектуальную обработку информации) и "разбирать" (извлекать конкретный контент из более крупного документа).

10.22 Средство или услуга, потребляющее контент MAEC, должно потреблять как минимум один тип выходного формата MAEC (связку, пакет или контейнер).

10.23 Средство или услуга, потребляющее контент MAEC, должно поддерживать разборку каждого типа выходного формата MAEC для извлечения любых вложенных типов, которые оно потребляет, независимо от местоположения этих типов выходного формата в документе в выходном формате. Например, средство или услуга, потребляющее только связки, должно быть в состоянии разбирать пакеты и контейнеры для извлечения контента связки.

10.24 Если средству или услуге требуется только информация технического анализа, связанная с образцом вредоносного программного обеспечения, то оно должно потреблять связки MAEC.

10.25 Если средству или услуге требуется информация технического анализа, связанная с образцом вредоносного программного обеспечения, а также метаданные для анализа и информация об отношении, то оно должно потреблять пакеты MAEC.

10.26 Если средству или услуге требуется информация технического анализа, связанная с несколькими наборами или группами образцов вредоносного программного обеспечения, оно должно потреблять контейнеры MAEC.

10.27 Если средство или услуга в процессе работы не потребляет файлы в выходном формате MAEC, то владелец возможности должен прописать процесс, с помощью которого пользователь может представить файлы в выходном формате MAEC владельцу возможности для интерпретации соответствующим средством или услугой. В документации должно быть указано, насколько быстро файлы, представленные владельцу возможности, будут доступны для данного средства или услуги.

11 Требования к органу по рассмотрению

Орган по рассмотрению должен соблюдать следующие требования, касающиеся совместимости с MAEC.

11.1 Орган по рассмотрению должен четко определять версию возможности, использованную для рассмотрения, версию документа требований к совместимости MAEC и версию языка MAEC, которая использовалась для определения формального соблюдения требований к совместимости с MAEC для каждой возможности.

11.2 Орган по рассмотрению должен определять тип(типы) функций возможности (создание контента, хранение контента или потребление контента).

11.3 Орган по рассмотрению должен определять и публиковать материалы теста выборки.

11.4 Орган по рассмотрению должен доводить до всеобщего сведения информацию о порядке участия в тестировании на правильность, с тем чтобы организации могли подготовиться как можно раньше.

11.5 Орган по рассмотрению должен сообщать контактное лицо для организации тестирования на правильность возможностей, заявленных как поддерживающие MAEC, по которым заполнена "Форма вопросника о совместимости с MAEC" .

11.6 Орган по рассмотрению, по собственному усмотрению, сможет провести повторное тестирование возможности, получившей официальное подтверждение о совместимости с MAEC.

12 Отзыв

Если орган по рассмотрению утвердил возможность как совместимую с MAEC, однако в дальнейшем у него появились доказательства, что установленные требования более не соблюдаются, то он может отозвать свое утверждение, и соответствующая возможность более не будет считаться имеющей официальное подтверждение о совместимости с MAEC. Ниже приводятся требования, которым должен следовать орган по рассмотрению, для того чтобы отозвать свое подтверждение.

12.1 Орган по рассмотрению должен предоставить владельцу возможности предупреждение об отзыве не позднее чем за два (2) месяца до даты планируемого отзыва.

12.2 Орган по рассмотрению может отложить дату отзыва.

12.3 Если орган по рассмотрению полагает, что действия или заявления владельца возможности являются заведомо вводящими в заблуждение, то он может не учитывать период предупреждения. Орган по рассмотрению может интерпретировать фразу "заведомо вводящими в заблуждение" по своему усмотрению.

12.4 Если орган по рассмотрению определяет, что действия владельца возможности в отношении требований к совместимости являются заведомо вводящими в заблуждение, то отзыв должен длиться не менее одного года.

12.5 Орган по рассмотрению должен определить конкретные требования, которые не соблюдаются.

12.6 Если владелец возможности полагает, что установленные требования соблюдены, он может ответить на предупреждение об отзыве, сообщив конкретные подробные данные, в которых указывается, почему соответствующая возможность удовлетворяет данным требованиям.

12.7 Если в течение периода предупреждения владелец возможности вносит изменения в соответствующую возможность с целью обеспечения ее соответствия установленным требованиям, орган по рассмотрению должен прекратить действия по отзыву в отношении этой возможности.

12.8 Орган по рассмотрению должен довести до всеобщего сведения, что официальное подтверждение правильности совместимости с MAEC в отношении соответствующей возможности отозвано.

12.9 Орган по рассмотрению может довести до всеобщего сведения причины такого отзыва.

Библиография

[b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2011 г.), *Общеизвестные уязвимости и незащищенность*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2014 г.