Международный союз электросвязи

МСЭ-Т

X.1126

(03/2017)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасные приложения и услуги – Безопасность подвижной связи

Руководящие указания по смягчению негативных последствий от зараженных терминалов в сетях подвижной связи

Рекомендация МСЭ-Т X.1126

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
Рекомендации, связанные с PKI	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальный транспортных системы (ИТС)	X.1370–X.1379
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.1126

Руководящие указания по смягчению негативных последствий от зараженных терминалов в сетях подвижной связи

Резюме

В Рекомендации МСЭ-Т X.1126 содержатся руководящие указания для операторов подвижной связи, призванные ограничить с помощью технологий использование зараженных терминалов в сетях подвижной связи, чтобы защитить как абонентов, так и операторов подвижной связи. В настоящей Рекомендации описываются характеристики и воздействие вредоносного программного обеспечения в нездоровой экосистеме в среде подвижной связи. В настоящей Рекомендации, основывающейся на сетевых технологиях, особое внимание уделяется смягчению негативного воздействия зараженных терминалов. В настоящей Рекомендации определяются и систематизируются меры по смягчению воздействия, а также соответствующие технологии.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1126	30.03.2017 г.	17-я	11.1002/1000/13194

Ключевые слова

Заражение, вредоносное программное обеспечение, сеть подвижной связи, терминал.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

© ITU 2017

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

Содержание

Введение

Быстрое распространение и развитие операционных систем мобильных устройств создало большой и динамичный рынок для отрасли подвижной связи. Для того чтобы воспользоваться возможностями этого ценного рынка, вокруг него возникло большое число экосистем. Однако вредоносное программное обеспечение также может использовать мощные возможности современных мобильных устройств для проникновения через уязвимости терминалов, а также сетей и услуг, вызывая значительный ущерб.

Необходимо отметить, что следует развивать здоровые экосистемы поверх традиционных систем подвижной связи, основанных на модели "огороженного сада", чтобы защитить рынок услуг подвижной связи и обеспечить выгоды для всех соответствующих партнеров. В ряде стран уже успешно реализованы здоровые экосистемы.

Отметим, что экосистемы рынка услуг подвижной связи в ряде странах весьма разнообразны, однако некоторые из них являются ненадежными, нездоровыми или даже опасными. Негативное воздействие ненадежных экосистем может нанести большой ущерб абонентам и сетям подвижной связи в дополнение к ущербу от вредоносного программного обеспечения. Иногда даже в условиях здоровой экосистемы абоненты и сети подвижной связи могут подвергаться негативному воздействию зараженных терминалов, так как большинство услуг мобильного интернета в настоящее время имеют глобальный охват.

Потенциальные риски распространения вредоносного программного обеспечения преимущественно в ненадежных экосистемах перечислены ниже.

Риски для абонентов:

- кража частной информации, например прослушивание и отслеживание местоположения;
- утрата ресурса, например нарушение работы системы, уничтожение данных;
- злонамеренные транзакции и потребление, такие как рассылка дорогостоящих сообщений, и набор номера центра обработки международных вызовов;
- распространение вредоносного программного обеспечения для атак на другие терминалы;
- рассылка спама, чтобы доставить неудобства другим абонентам;
- мошенничество и шантаж.

Риски для операторов, атаки на сетевые объекты, услуги подвижной связи и другие терминалы, в том числе:

- загрузка крупных ресурсов сетей и услуг подвижной связи, которая приводит к нарушению их нормального функционирования и жалобам абонентов на качество обслуживания;
- установление контроля над узлами предоставления услуг и даже сетевыми объектами.

Вредоносное программное обеспечение приносит больший ущерб мобильному интернету, чем традиционному проводному интернету по следующим причинам:

- рынок мобильного интернета является развивающимся рынком, что характеризуется относительно медленным развитием соответствующих механизмов обеспечения безопасности;
- мобильные терминалы зачастую содержат информацию частного и конфиденциального делового характера, которая является весьма привлекательной мишенью для хакеров;
- сети подвижной связи имеют меньше ресурсов, а флуд-атака загружает эти ресурсы значительно проще и в больших объемах;
- многие мобильные терминалы прочно соединены со своими сетями; вредоносные услуги и кражи частной информации могут привести к потере доходов оператора, жалобам абонентов и юридическим проблемам;
- открытая или взломанная мобильная операционная система создает не поддающиеся контролю операторов условия для распространения вредоносного программного обеспечения;
- мобильные терминалы часто имеют несколько интерфейсов для обмена данными, например универсальная последовательная шина (USB), слот защищенной цифровой (SD) карты и Bluetooth, поэтому операторы не могут обеспечить защитой многие из них.

Для того чтобы смягчить ущерб от вредоносного программного обеспечения и отслеживать источники угроз, жизненно важно осуществлять управление зараженными терминалами на стороне сети, что составляет ответственность и обязанность операторов подвижной связи.

Рекомендация МСЭ-Т X.1126

Руководящие указания по смягчению негативных последствий от зараженных терминалов в сетях подвижной связи

1 Сфера применения

В настоящей Рекомендации содержатся руководящие указания по смягчению с помощью сетевых технологий негативных последствий от зараженных терминалов в сетях подвижной связи. Структура настоящей Рекомендации выбрана таким образом, чтобы упорядочить эти руководящие указания в соответствии с процессами. Кроме того, в настоящей Рекомендации обсуждаются принципы, политика и технологии, используемые в этих процессах.

Соответствие настоящей Рекомендации не следует рассматривать в качестве какого-либо доказательства заявленного соблюдения любых национальных или региональных законов, норм или политики. Описанные в настоящей Рекомендации технические, организационные и процедурные средства ни в коей мере не гарантируют создания какого-либо уровня безопасности, который может налагаться на определенную корреспонденцию в соответствии с конкретным национальным или региональным законом, нормой или политикой.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 черный список (blacklist) [b-ITU-T X.1245]: Список с идентификацией для лиц или источников в услугах связи, где для получения доступа к определенным ресурсам связи идентификации, включенные в список, отклоняются.

3.1.2 вредоносное программное обеспечение (malware) [b-ITU-T X.1211]: Вредоносное программное обеспечение, предназначенное специально для повреждения или разрушения системы путем нарушения конфиденциальности, целостности и/или доступности.

ПРИМЕЧАНИЕ. – К примерам относятся вирусы, программы-вымогатели, программы-шпионы, программы, содержащие рекламу или поддельные антивирусы.

3.1.3 сеть подвижной связи (mobile network) [b-ITU-T X.1121]: Сеть, которая предоставляет мобильным терминалам пункты доступа к беспроводной сети.

3.1.4 мобильный терминал (mobile terminal) [b-ITU-T X.1121]: Объект, который имеет функцию доступа к беспроводной сети и соединяет подвижную сеть передачи данных с серверами приложений или другими мобильными терминалами.

3.1.5 спамминг (spamming) [b-ITU-T X.1244]: Последовательность действий, выполняемых спаммером для рассылки спама. Например, сбор списков целевой рассылки, создание спама, доставка спама и т. д.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин:

3.2.1 бот-сеть (botnet): Группа взломанных компьютерных систем, которые заражены вредоносным программным обеспечением и соединены скоординированным образом для достижения злонамеренных целей без ведома их владельцев, например для передачи вредоносного программного обеспечения либо спама, либо для начала атак.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

App	Application running on mobile terminals	Приложение, работающее на мобильных терминалах
API	Application Programming Interface	Интерфейс прикладного программирования
C& C	Command and Control	Управление и контроль
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
GGSN	Gateway General packet radio service Support Node	Шлюзовой узел поддержки службы пакетной радиосвязи общего пользования
IP	Internet Protocol	Протокол Интернет
MMS	Multimedia Messaging Service	Услуга передачи мультимедийных сообщений
MMSC	Multimedia Messaging Service Centre	Центр услуг передачи мультимедийных сообщений
SD	Secure Digital	Защищенный цифровой
SIM	Subscriber Identity Module	Модуль идентификации абонента
SMS	Short Message Service	Услуга передачи коротких сообщений
SMSC	Short Message Service Centre	Центр услуг передачи коротких сообщений
URL	Uniform Resource Locator	Универсальный указатель ресурса
USB	Universal Serial Bus	Универсальная последовательная шина
VAS	Value-Added Service	Дополнительные услуги
WAP	Wireless Application Protocol	Протокол беспроводных приложений

5 Условные обозначения

Отсутствуют.

6 Структура и процессы

В большинстве случаев после заражения вредоносным программным обеспечением большинство мобильных терминалов все еще могут получать доступ к сетям и пользоваться, как обычно, всеми возможными услугами, но при этом начинается также негативное воздействие на сети и услуги, о чем абоненты могут и не знать. Оператор подвижной связи обязан знать о заражении и ограничить надлежащим образом работу зараженного терминала, с тем чтобы сохранить стабильность возможностей своей сети и услуг и поддерживать доверие к ней, защищая благоприятные условия работы абонентов. На Рисунке 1 представлена структура смягчения негативных последствий в тех случаях, когда существуют три типа ролей: операторы, абоненты и другие организации. Операторы играют ключевую роль в этой структуре и их работу можно подразделить на три процесса: выявление, управление и обмен информацией. В целях содействия этим трем процессам в структуру включена база данных вредоносного программного обеспечения и вредоносных источников. Операторы осуществляют процессы в рамках этой структуры с учетом национальных правовых и регуляторных обязательств конкретных Государств-Членов, в которых они работают.

Между тремя ролями существуют взаимоотношения: операторы выявляют аномалии терминалов абонентов с помощью сетевых технологий и управляют этими аномалиями, а затем они информируют абонентов об угрозах, которые представляют эти аномалии. Далее операторы могут также передать информацию о вредоносном программном обеспечении сотрудничающим с ними операторам и организациям.

В рамках процесса выявления можно собрать и проанализировать образцы используемых в мобильных терминалах приложений и отчеты об атаках для того, чтобы выявить аномалии в сети подвижной связи. В рамках процесса управления составляется отчет об аномалиях и затронутых терминалах. В рамках процесса управления происходит подтверждение аномалий и принимаются особые меры по смягчению негативных последствий для абонентов и операторов. С целью предоставить вовремя информацию для противодействия вредоносному программному обеспечению либо чтобы справиться с возникающими проблемами, необходимо установить процесс обмена информацией. Процесс обмена информацией подразумевает передачу информации о вредоносном программном обеспечении сотрудничающим операторам и организациям в целях повышения безопасности всей отрасли.

База данных вредоносного программного обеспечения и вредоносных источников: все процессы замкнуты на базу данных вредоносных программ и источников для хранения и использования сведений о таких кодах, в том числе о моделях их поведения и их источниках. Сведения содействуют выявлению аномалий, контролю над зараженными терминалами и публикации информации о вредоносном программном обеспечении в рамках трех процессов. Кроме того, новые сведения о вредоносном программном обеспечении, поступившие в результате процесса выявления и обмена информацией, могут использоваться для обновления базы данных в целях реализации постоянно актуальной защиты.

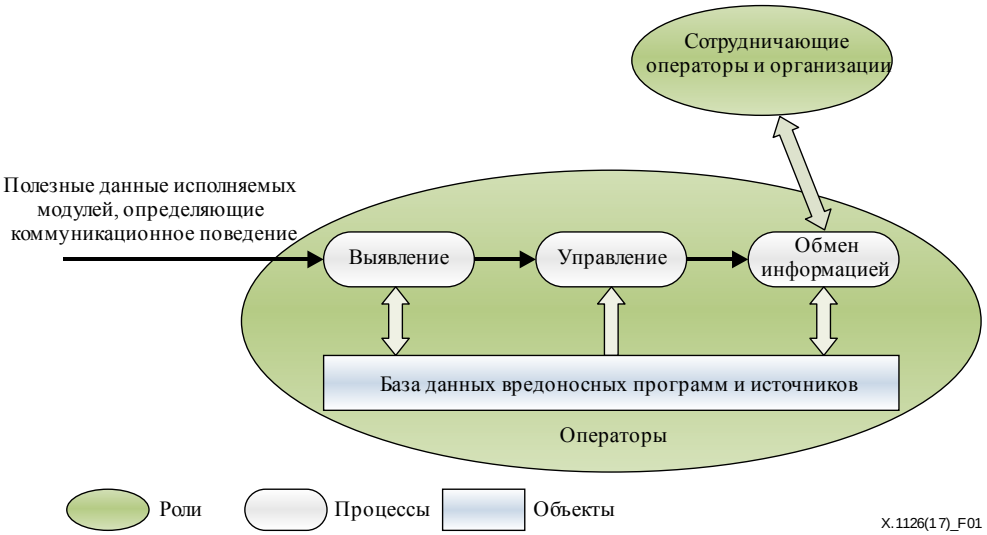

Рисунок 1 – Структура смягчения негативных последствий от зараженных терминалов

7 Выявление

В рамках процесса выявления происходит сбор образцов приложений из магазинов приложений и отчетов об атаках, отправленных и терминалами, и сетевыми элементами, в целях анализа аномалий сети подвижной связи, которые могут быть индикаторами либо признаками зараженных терминалов и вредоносных источников. На Рисунке 2 представлена схема процесса выявления.

Все данные, используемые в данном и последующих разделах, могут быть собраны на основании образцов приложений из магазинов, а также отчетов об атаках, отправленных терминалами абонентов либо сетевыми элементами. В процессе выявления любое использование данных может быть связано с неприкосновенностью частной информации абонента, и может потребоваться согласие либо разрешение абонента в соответствии с местным законодательством. Использование данных должно строго ограничиваться анализом вредоносной программы и связанной с ней деятельностью и ничем более.

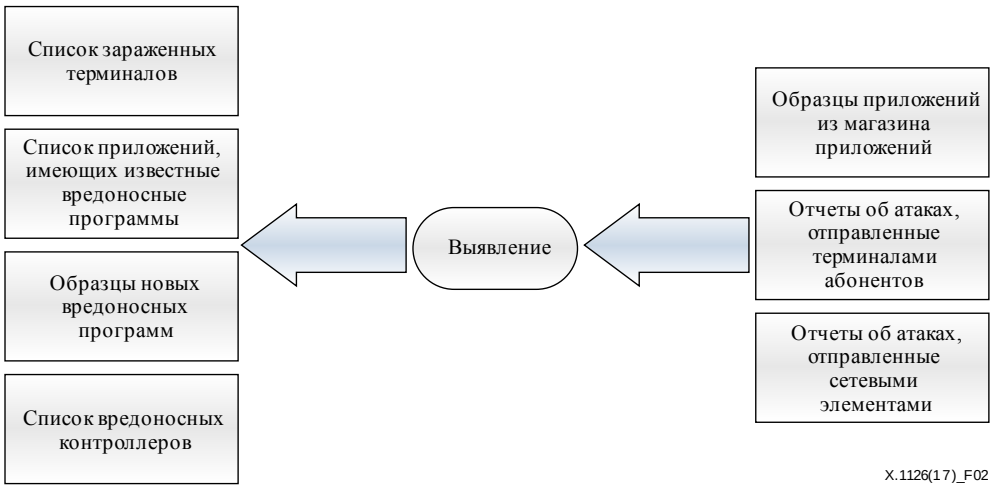

Рисунок 2 – Интерактивные взаимоотношения в рамках процесса выявления

7.1 Сбор приложений и отчетов об атаках

В рамках процесса выявления может осуществляться сбор двух видов данных для определения характеристик сетевых аномалий:

- отчеты об атаках, полученные от терминалов абонентов и сетевых элементов;
- образцы приложений из магазинов/рынков приложений.

7.2 Анализ зараженных терминалов и известного вредоносного программного обеспечения

Некоторые зараженные терминалы могут быть выявлены на основе отчетов об атаках. Дополнительное сопоставление сигнатур может помочь найти новые приложения, которые содержат известное вредоносное программное обеспечение.

Анализ зараженных терминалов и известного вредоносного программного обеспечения применяется для определения местоположения скрывающихся в сети вредоносных контроллеров.

Адреса протокола Интернет (IP), содержащиеся в управляющих пакетах зараженных терминалов, необходимо проанализировать, чтобы определить IP-источники, которые управляют зараженными терминалами либо собирают данные о состоянии зараженных терминалов.

Необходимо проводить динамический анализ в отношении известного вредоносного программного обеспечения, которое найдено в приложениях, чтобы проверить наличие каких-либо обновлений у вредоносных контроллеров.

7.3 Анализ нового вредоносного программного обеспечения

Основываясь на приложениях, полученных из магазинов приложений, новое вредоносное программное обеспечение может быть выявлено с помощью статического и динамического анализа модели поведения,.

7.3.1 Вредоносные коды и анализ исполняемых модулей

Статический анализ: этот подход используется для понимания на синтаксическом уровне подозрительного вредоносного программного обеспечения. Например, мобильное приложение может быть разобрано с помощью технологии реверсивного проектирования, чтобы получить файл манифеста (содержащий информацию о разрешениях на доступ, которые имеет приложение), а также исходные коды. С помощью изучения файла манифеста и сканирования характеристик вызова интерфейса прикладного программирования (API) можно распознать ряд злонамеренных попыток с помощью типовых принципов обнаружения:

- имеется какая-либо излишня и важная привилегия доступа;
- вызывается API сети для доступа к вредоносным интернет-источникам;
- вызывается API процесса для завершения работы приложения;

- вызывается API процесса для экспорта контактной информации на конкретный адрес;
- имеет место необычная модель поведения при чтении защищенной цифровой (SD) карты (памяти) либо карты модуля идентификации абонента (SIM);
- происходит обмен данными с известным вредоносным универсальным указателем ресурса (URL);
- имеется подписка на услугу передачи коротких сообщений (SMS) без запроса абонента;
- имеются какие-либо инструкции по дистанционному управлению мобильным терминалом.

Динамический анализ: этот подход предусматривает работу с вызывающим подозрение вредоносным программным обеспечением для мобильных устройств и наблюдение за его работой в контролируемой (и даже виртуализированной) среде (например, в изолированной среде). Далее приводятся некоторые типовые принципы обнаружения:

a) Соединение с бот-сетью

i) Описание: бот должен сообщить о своем существовании серверу управления и контроля (C&C) для соединения с бот-сетью, а сервер C&C дает указание бот-сети приступить к вредоносной деятельности. Сервер C&C может быть веб-сервером либо терминалом сети подвижной связи, при этом инструкция может быть дана с использованием услуг интернета, SMS или передачи мультимедийных сообщений (MMS).

ii) Принципы обнаружения:

1) большое количество терминалов соединяется с известным вредоносным хостом;

2) терминал соединяется с известным вредоносным хостом периодически и на продолжительное время;

3) терминал отправляет двоичные SMS сообщения большому числу терминалов.

b) Распространение и спамминг

i) Описание: вредоносное программное обеспечение распространяется самостоятельно либо максимально широко отправляет спам другим абонентам с помощью других услуг (интернет, MMS, SMS, и т. д.).

ii) Принципы обнаружения:

1) большое количество терминалов отправляют одни и те же сообщения MMS или SMS (сообщения сравниваются с односторонней хэш-функцией), а географическое распределение осуществляется произвольно;

2) объем услуг резко возрастает в период простоя;

3) осуществление трехсторонних вызовов;

4) отправка сообщений SMS;

5) отправка сообщений MMS;

6) программное обеспечение активирует провоцирующий вызов;

7) информация в SIM-карте экспортируется на сервер с помощью программного обеспечения;

8) через короткий промежуток времени программное обеспечение активирует вредоносный вызов;

9) происходит ненужная дополнительная загрузка;

10) доступ к известным вредоносным контроллерам.

c) Вредоносные подписки и потребление

i) Описание: зараженные терминалы будут подписываться на дополнительные услуги (VAS) и на услуги трехсторонних вызовов, чтобы осуществлять вызовы с оплатой по повышенному тарифу либо международные вызовы, а также рассылать большое количество сообщений. Абонент не будет знать об этих платах.

ii) Принципы обнаружения:

1) необъяснимый рост счетов абонента;

2) зараженный терминал часто совершает вызовы с оплатой по повышенному тарифу либо международные вызовы в определенные периоды времени;

3) многочисленные терминалы постоянно отправляют одни и те же сообщения множество раз в определенные периоды времени;

4) терминал подписывается на услуги тройных вызовов и часто, и даже постоянно, их использует.

d) Атака на основе распределенного отказа в обслуживании (DDoS):

i) Описание: множество терминалов перегружают радио- и иные ресурсы сети подвижной связи, чтобы снизить качество обслуживания.

ii) Принципы обнаружения:

1) резко возрастает трафик в шлюзовом узле поддержки службы пакетной радиосвязи общего пользования (GGSN) либо в других сетевых объектах, при том что бóльшая часть трафика имеет одинаковое место назначения.

Статический анализ не применим в отношении подпадающего под подозрение вредоносного программного обеспечения, которое скрыто либо является намеренно запутанным, а динамический анализ не может охватить полностью весь программный код. Поэтому следует проводить как статический, так и динамический анализ, чтобы составить представление о том, как функционирует это конкретное вредоносное программное обеспечение.

Попытки необычных действий либо необычные модели поведения, которые были зафиксированы и распознаны с помощью статического и динамического анализа, будут полезны для уточнения принципов анализа модели поведения в отношении последних по времени аномальных сценариев. Более того, эти распознанные характеристики могут также помочь операторам найти неизвестные вредоносные URL либо IP-адреса.

7.3.2 Комбинированный подход

В связи с этим предлагается объединить два аналитических подхода для улучшения показателей работы и сокращения количества ложноположительных результатов в процессе выявления.

В процессе выявления могут быть получены различные результаты, содействующие процессу управления. Результаты процесса выявления включают, в том числе:

- список зараженных терминалов;
- образцы приложений, содержащих известное вредоносное программное обеспечение;
- образцы нового вредоносного программного обеспечения;
- список вредоносных контроллеров.

Вышеуказанная информация является важной для операторов для принятия надлежащих мер в процессах, которые описаны в разделах 8 и 9.

8 Управление

В процессе управления автоматически либо полуавтоматически анализируются и подтверждаются результаты процесса выявления. Далее принимаются меры по управлению в соответствии со степенью аномалии. На Рисунке 3 представлена схема интерактивных взаимоотношений между процессом управления и другими сетевыми объектами и объектами обслуживания.

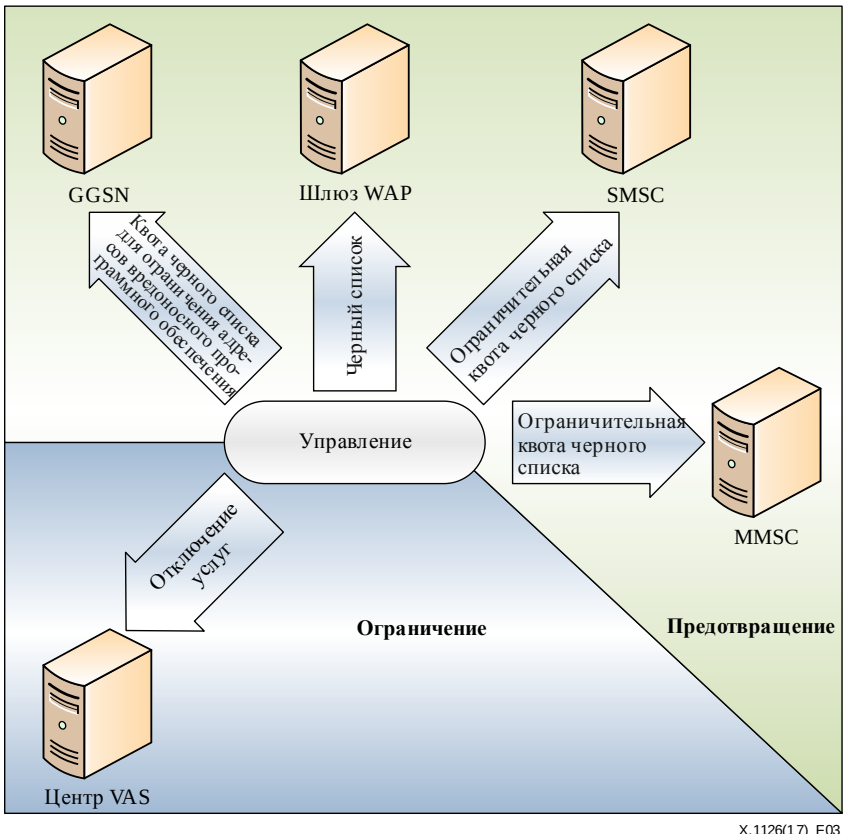

Рисунок 3 – Интерактивные взаимоотношения в рамках процесса управления

8.1 Меры по управлению

Существуют два вида мер, связанные с различной сложностью аномалий: предотвращение и ограничение, оба из которых используют возможности сетевых объектов и платформ, поддерживающих услуги.

- Предотвращение: если аномалия является умеренной и ее можно контролировать не прерывая предоставление предлагаемых абонентам услуг, для решения проблемы можно использовать метод предотвращения.
- Ограничение: если подход на основе предотвращения не работает, и абоненту уже нанесен существенный финансовой ущерб, вводится ограничение для частичной либо полной приостановки подвергшихся воздействию услуг.

8.2 Предотвращение

8.2.1 Черный список

В тех случаях, когда аномалия является результатом действий вредоносного контроллера, то контроллер может быть добавлен в черный список. После этого любые последующие запросы к этому контроллеру либо от него будут заблокированы. Многие сетевые объекты, например GGSN, шлюз протокола беспроводных приложений (WAP) и центр услуг передачи мультимедийных сообщений (MMSC), поддерживают функцию черного списка. Существует возможность ведения нескольких черных списков для блокирования различных видов вредоносных контроллеров, например списки имен доменов вредоносных веб-сайтов, и IP-адресов серверов C&C. Необходимо отметить, что источники в черном списке необходимо регулярно подтверждать и уточнять, чтобы не допустить блокирования законных источников.

Любые адреса, которые связаны с загрузкой каких-либо приложений, содержащих вредоносное программное обеспечение, могут быть заблокированы с помощью GGSN.

8.2.2 Ограничительная квота

В тех случаях, когда спам-деятельность является основной причиной аномалии в сети, например атака DDOS, для снижения скорости распространения может быть использован подход на основе ограничительной квоты. Ограничительная квота определяет порог для максимального количества сообщений, которые могут быть отправлены в определенный период времени (например, за месяц) с полной гарантией возможностей любого терминала обеспечить базовую связь или связь в чрезвычайных ситуациях. Когда количество сообщений превышает определенный порог, налагается запрет на отправку большего количества сообщений.

8.3 Ограничение

8.3.1 Отключение услуг оператора

Если вредоносный контроллер находится в услуге оператора, что может произойти в результате взлома, оператор может использовать свое право и выполнить свое обязательство и отключить временно свою собственную услугу и использовать резервную услугу, если необходимо выполнить обязательство по предоставлению услуг связи в чрезвычайных ситуациях.

9 Обмен информацией

Управление не может быть конечной целью, поскольку оно пытается лишь свести к минимуму негативное воздействие на абонентов и на сети. Конечной целью является восстановление нормальной работы и предотвращение более широкого заражения. Поэтому процесс обмена информацией важен для совершенствования всей структуры.

Чтобы улучшить состояние отрасли, операторами будет осуществляться только обмен образцами вредоносного программного обеспечения.

Необходимо отметить, что процесс обмена информацией должен соответствовать местному законодательству и абонентским контрактам.

Библиография

[b-ITU-T X.1121] Рекомендация МСЭ-Т X.1121 (2004 г.), *Структура технологий безопасности для подвижной передачи данных от конца до конца*.

[b-ITU-T X.1211] Рекомендация МСЭ-Т X.1211 (2014 г.), *Методы предотвращения атак на базе веб-сети*.

[b-ITU-T X.1244] Рекомендация МСЭ-Т X.1244 (2008 г.), *Общие аспекты противодействия спаму в мультимедийных IP-приложениях*.

[b-ITU-T X.1245] Рекомендация МСЭ-Т X.1245 (2010 г.), *Структура противодействия спаму в мультимедийных IP-приложениях*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2017 г.