МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННЫХ С ФУНКЦИОНИРОВАНИЕМ СКРЫТЫХ ВО ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММАХ

***Барабанов Александр Владимирович**, кандидат технических наук*
Гришин Максим Иванович
Кубарев Алексей Валентинович

Основной задачей настоящей статьи является определение основных угроз безопасности информации, содержащейся в информационных системах, связанных с руткитами. Указанные угрозы определяются впервые. Для решения указанной задачи описываются основные методы реализации главной функции руткитов, перечисляются их дополнительные функциональные возможности, рассматриваются способы их распространения и определяются уязвимости программного обеспечения, эксплуатируемые для внедрения руткитов.

***Ключевые слова**: руткит, безопасность информации, информационные системы, угрозы безопасности информации, моделирование угроз.*

MODELING OF INFORMATION SECURITY THREATS CAUSED BY ROOTKITS

***Alexander Barabanov**, Ph.D*
Maksim Grishin
Alexey Kubarev

The main objective of this article is determination of the most possible threats of information security, containing in information systems, caused by rootkits. These threats determined for the first time. There are the most methods of realization of main rootkit function are describing, additional rootkit functionality is listing, rootkit distribution methods are considered and software vulnerabilities that are exploitable for rootkit loading into information system are determining in this article for solving the objective.

***Keywords**: rootkit, information security, information systems, information security threats, threat modeling.*

Одним из основных источников угроз безопасности информации (БИ) является вредоносное программное обеспечение, в том числе компьютерные вирусы, трояны, черви, целенаправленные вредоносные программы и т. д. Технологии, используемые злоумышленниками для нарушения БИ не стоят на месте, и все большее распространение получает технология, обеспечивающая скрытое функционирование вредоносного программного обеспечения – руткит: в соответствии с исследованиями [1] за последние годы (рис. Рис. 1) наблюдается устойчивый рост числа выявляемых руткитов. В первую очередь указанная технология направлена на скрытие своих и прочих объектов от средств антивирусной защиты, и сама по себе не направлена на нанесение вреда безопасности информации информационной системе, поэтому угрозы, связанные с ней нецелесообразно относить к угрозам, связанным с вредоносным программным обеспечением. Из-за того, что ключевая функция руткитов – сокрытие факта собственного наличия в системе и следов собственного функционирования, довольно сложно оценить реальное количество существующих на данный момент объектов указанного класса, но, в соответствии с отчетом лабораторий McAfee по угрозам за июнь 2014 г., общее количество руткитов постоянно активно растет.

В настоящее время поставщиками и разработчиками предлагается целый ряд средствам защиты информации (СЗИ), которые могут применяться в информационной системе (ИС) для парирования данной угрозы (средства антивирусной защиты), однако требования к таким средствам защиты отсутствуют, что не позволяет обеспечить их качественную сертификацию и последующее применение [2].

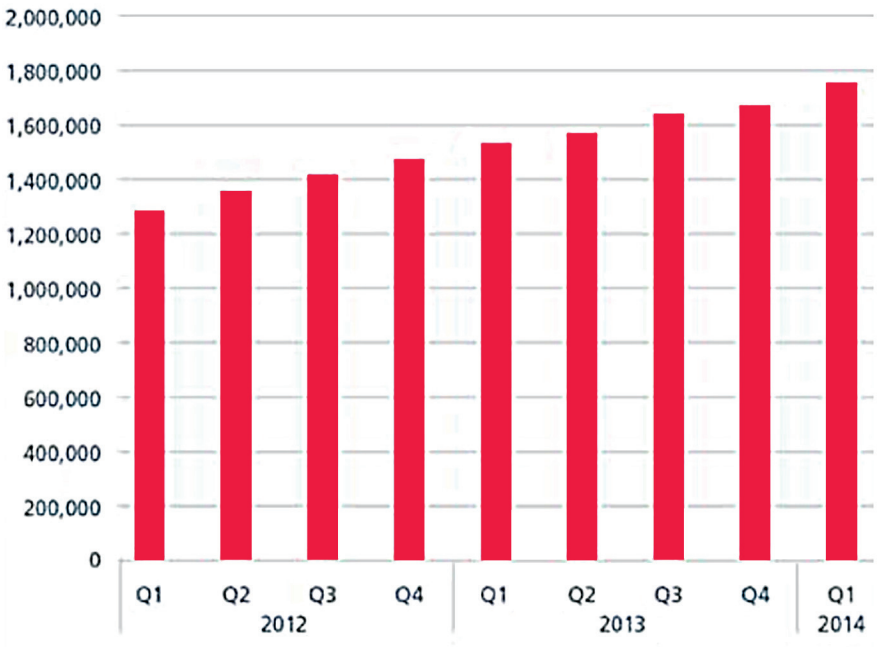

Рис. 1. *Число выявленных скрытых в операционной системе вредоносных компьютерных программ (руткитов)*

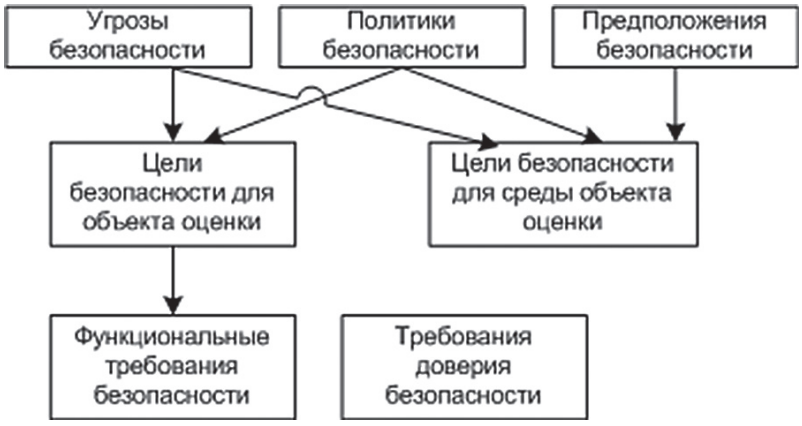

Рис. 2*. Последовательность формирования ФТБ и ТДБ*

Формирование требований БИ целесообразно выполнять в соответствии с последовательностью, предлагаемой методологией «Общих критериев»[1]. На рисунке 2 представлена последовательность формирования функциональных требований безопасности (ФТБ) и требований доверия к безопасности (ТДБ) для объекта оценки (ОО, в данном случае – средство антивирусной защиты).

Изложение среды безопасности объекта оценки должно содержать описание аспектов безопасности среды, в которой предполагается использовать ОО, и ожидаемый способ его применения. Это изложение должно включать:

- описание предположений безопасности, содержащее аспекты безопасности среды, в которой будет использоваться ОО или предполагается к использованию;
- описание угроз, включающее все те угрозы активам, против которых требуется защита средствами ОО или его среды;
- описание политики безопасности организации, идентифицирующее и, при необходимости, объясняющее все положения политики безопасности организации или правила, которым должен подчиняться ОО.

Цели безопасности должны отражать изложенное намерение противостоять всем установ-

1 ISO/IEC 15408-1:2009. Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model.

ленным угрозам и быть подходящими для этого, а также охватывать все предположения безопасности и установленную политику безопасности организации. Цели безопасности для ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым необходимо противостоять средствами ОО, или с политикой безопасности организации, которой должен отвечать ОО. Цели безопасности для среды ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым не полностью противостоит ОО, или с политикой безопасности организации и предположениями, не полностью удовлетворяемыми ОО. При изложении требований безопасности ОО должны быть определены функциональные требования и требования доверия, которым должны удовлетворять ОО.

Именно правильное определение множества угроз БИ является необходимым условием формирования множества ФТБ. Таким образом, задача моделирования угроз БИ, связанных с функционированием скрытых вредоносных компьютерных программ (руткитов), является актуальной.

Под угрозой БИ целесообразно понимать совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в информационной системе. В [3] показано, что в описание угрозы БИ должны входить элементы, представленные на рисунке 3.

Далее рассмотрены особенности функционирования руткитов и представлены результаты моделирования угроз БИ.

Скрытое функционирование на инфицированных вычислительных устройствах руткитов (или другого вредоносного программного обеспечения), обеспечивается путем применения различных методов, основанных на особенностях архитектуры операционных систем и недостатках средств защиты информации. Первоначально руткиты создавались для Unix-систем, при этом использовались примитивные способы скрытия в системе, такие как замена системных файлов вредоносными версиями, что легко обнаруживалось путем сканирования файлов. С течением времени, техники, которые используются в рукткитах, стали затрагивать недокументированные структуры операционных систем и даже аппаратную составляющую технических средств [4].

Одним из первых способов скрытия вредоносной программы была замена системного файла на вредоносный файл с таким же именем и функциями, что и оригинальный файл. Например, заменяется компонент операционной системы (ОС), который отвечает за отображение списка файлов в директории, на компонент, обеспечивающий фильтрацию выводимых данных и не отображающий вредоносные файлы, присутствующие в системе. Такие вредоносные программы легко обнаруживаются с использованием средств обеспечивающих контроль целостности системных файлов.

Другой способ, применяемый руткитами, это различные перехваты («hook»). Перехват - это метод, используемый в программировании для изменения поведения какой-либо системной функции путем подмены указателя на какой-либо ресурс или функцию, используемую в нормальном режиме работы, указателем на другую функцию или ресурс. При этом изменение файлов на диске не происходит, поэтому обнаружение путем проверки целостности файлов не даст результата.

Перехваты реализуются модификацией различных структур данных операционных систем: таблица импорта (Import Address Tables), таблица описателей прерываний (Interrupt Descriptor Table), таблица диспетчеризации сервисов (System Service Dispatch Table), пакеты запросов ввода-вывода (I/O Request Packets) для операционных систем семейства Windows или таблица системных вызовов, таблица описателей прерываний инструкции sysenter/syscall через специфичные

Угроза БИ: = <аннотация угрозы>, <источник угрозы>, <способ реализации угрозы>, <используемые уязвимости>, <вид информационных ресурсов, потенциально подверженных угрозе>, <нарушаемое свойство безопасности информационных ресурсов>,<возможные последствия реализации угрозы>

Рис. 3. *Структура описания угроз БИ, связанных с применением скрытых в операционной системе вредоносных компьютерных программ (руткитов)*

для процессора регистры для операционных систем семейств Unix/Linux [5]. Указанные структуры обычно содержат множество адресов в памяти, которые указывают на различные системные функции и процедуры обработки, которые могут быть изменены и будут в этом случае указывать на функции и процедуры вредоносного программного обеспечения.

Существуют руткиты, использующие в своей работе технику Direct Kernel Object Manipulation, которая подразумевает выполнение различных действий со структурами ядра операционной системы для того, чтобы скрыть процессы, изменить привилегии и т.п. Например, в операционной системе Windows для сокрытия вредоносных процессов может быть использован двунаправленный список EPROCESS, в ОС Linux – внутренний список модулей, содержащий ссылки на все модули, загруженные в систему.

Еще одним способом, применяемым разработчиками руткитов, является внесение изменений в системные процедуры, что позволяет выполнить вредоносный код, который располагается на диске или в оперативной памяти. Для перенаправления потока исполняемых команд используется внедрение инструкций, таких как JMP, в код системных процедур. Изменения вносятся в системные файлы ОС, что легко обнаруживается путем сигнатурного анализа файлов, либо в исполняемый код, который уже находится в оперативной памяти, что делает обнаружение затруднительным [5].

Характерным для ОС Windows и распространенным способом скрытия присутствия вредоносных файлов в системе является использование драйверов-фильтров. Драйвер-фильтр – специальный драйвер, предназначенный для расширения функциональности обычных драйверов устройств или изменения поведения устройства в системе. Использование таких драйверов предусмотрено архитектурой ОС Windows. Использование таких драйверов позволяет разработчикам руткитов внедрять вредоносный код для перехвата пакетов запросов ввода-вывода и проводить такие действия, как запись нажатий клавиш, фильтрация результатов обработки прерываний, возвращаемых антивирусному программному обеспечению. Используя драйверы-фильтры можно выполнять перехваты драйверов, внесение изменений в функции драйверов [5].

Существует возможность создания руткитов использующих аппаратную виртуализацию или уязвимости чипсетов материнских плат и работающих на уровне BIOS или расширений PCI-карт. Однако, на текущий момент, данные типы руткитов очень редки и на практике не применяются, т. е. существуют только на уровне идей [6-9].

Итак, к наиболее распространенным методам маскирования функционирования руткитов относятся:

- маскировка объектов, содержащих вредоносный код, под обычные объекты операционной системы или программного обеспечения;
- использование «перехватов» - техники, которая используется для изменения нормального поведения системных функций;
- манипулирования объектами ядра ОС (DKOM);
- внесение изменений в системные процедуры ОС («patching»);
- применение драйверов-фильтров в ОС Microsoft Windows.

Руткит может быть направлен на сокрытие установки и функционирования вредоносного программного обеспечения, не входящего в его состав, но, как правило, код руткита снабжается некоторой «полезной нагрузкой» (функциональными возможностями), решающей прикладные задачи вредоносного характера.

Такие функции, как правило, являются вредоносными и к ним относятся:

- загрузка и исполнение прочего вредоносного программного обеспечения;
- автоматизированный перехват данных, вводимых пользователем на инфицированном устройстве и их регистрация;
- сигнатурный анализ информации, содержащейся на инфицированном устройстве;
- сбор информации о параметрах информационной системы, в состав которой входит инфицированное устройство и её регистрация;
- удаленный доступ к инфицированному устройству с целью управления им;
- копирование и (или) передача данных, содержащихся на инфицированном устройстве во внешнюю среду;
- нарушение целостности информации, содержащейся в инфицированном устройстве;
- нарушение работоспособности компонентов инфицированного устройства;
- использование ресурсов инфицированного устройства для осуществления вредоносной деятельности вовне (в т. ч., для рассылки нежелательных почтовых сообщений, перебора паролей, осуществления распределенных атак типа «отказ в обслуживании» и т. п.);
- саморепликация;
- распространение собственных копий.

Таким образом, руткит, как правило, реализует одновременно две функции: сокрытие факта своего присутствия на инфицированном устройстве и при этом реализация некоторых вредоносных воздействий на инфицированное устройство.

Способы внедрения руткитов не отличаются от способов внедрения прочих классов вредоносного программного обеспечения. Внедрение руткита в информационную систему может производиться путем использования каналов передачи данных, связывающих информационную систему с другими информационными системами, в том числе через сети связи общего пользования, либо путем использования отчуждаемых носителей информации.

Почтовые сообщения могут являться нежелательными и рассылаться в автоматизированном режиме (т. е. представляют собой «спам») или, например, направляться определенным лицами или группам лиц. Электронное почтовое сообщение, отправляемое с целью атаки, может содержать следующие данные, обеспечивающие установку руткита в систему: ссылка на файл, содержащий руткит; ссылка на сценарий, который обеспечивает копирование и установку руткита в системе; вложенный файл, содержащий руткит или ссылку на него; вложенный файл, содержащий сценарий, который обеспечивает копирование и установку руткита в системе, или ссылку на такой сценарий.

Файлы, необходимые для установки руткита могут содержаться на отчуждаемых носителях. При подключении носителя к техническим средствам информационной системы осуществляется автоматическая установка руткита в систему. Распространение совместно с программным обеспечением или компонентами программного обеспечения, которое необходимо для выполнения устройством каких-либо функций, либо запускается несанкционированно на устройстве пользователями.

Руткит может быть установлен на устройство совместно с программным обеспечением, которое устанавливается или запускается пользователями. При этом файлы, необходимые для установки программного обеспечения обычно копируются через сети связи общего пользования, либо поступают на отчуждаемых носителях.

Установка руткита может быть осуществлена в процессе получения доступа пользователя к вредоносному, взломанному или скомпрометированному веб-ресурсу. При этом сценарии, размещенные на таком ресурсе, используют уязвимости программного обеспечения информационной системы для копирования и установки руткита.

В случае неавтоматизированной установки руткита в процессе осуществления целевой компьютерной атаки, руткит устанавливается непосредственно злоумышленником после осуществления им успешной компьютерной атаки на информационную систему, целью которой являлось получение повышенных привилегий, необходимых для установки руткита.

Для осуществления компьютерной атаки злоумышленником используются различные уязвимости в программном обеспечении информационной системы, а также методы социальной инженерии.

Таким образом, передача руткитов цели обычно производится при помощи:

- электронных почтовых сообщений, содержащих инфицированное вложение;
- отчуждаемых носителей, содержащих инфицированные файлы;
- инфицированного программного обеспечения;
- полученных злоумышленником необходимых привилегий.

При проведении атак, в том числе результатом которых является внедрение руткитов, злоумышленники обычно используют уязвимости следующего программного обеспечения: браузеры различных производителей, Oracle Java, Adobe Reader, AndroidOS, Adobe Flash Player, Microsoft Office. На рисунке 4 приведено распределение эксплуатируемых в ходе атак уязвимостей по типу программного обеспечения.

Далее представлено краткое описание уязвимостей, которые могут эксплуатироваться в процессе внедрения руткитов в информационную систему.

Наиболее опасным типом эксплуатируемых уязвимостей является наличие в приложении некорректных операций с памятью (переполнение буфера), которые обычно возникают при возникновении следующих условий:

- обращение к несуществующему объекту в памяти;
- операция разыменования недействительного указателя;
- обращение к элементу массива по индексу, выходящему за границы массива.

Наиболее опасным типом эксплуатируемых уязвимостей является наличие в приложении некорректных операций с памятью (переполнение буфера), которые обычно возникают при возникновении следующих условий: обращение к несуществующему объекту в памяти, операция

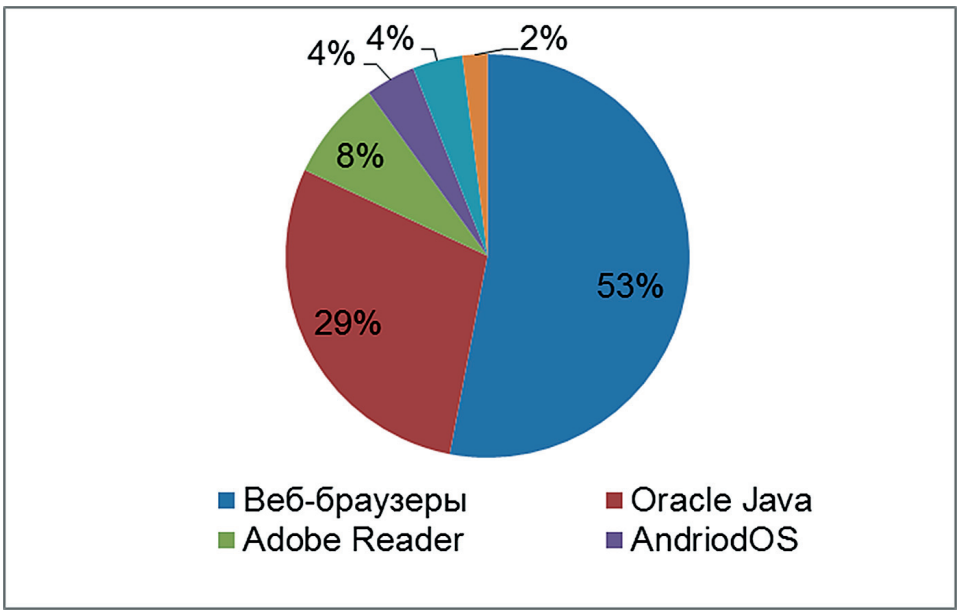

Рис. 4. *Распределение эксплуатируемых в ходе атак уязвимостей по типу программного обеспечения*

разыменования недействительного указателя, обращение к элементу массива по индексу, выходящему за границы массива и т. п. Уязвимости данного типа являются критическими уязвимостями программного обеспечения и позволяют нарушителю выполнить повышение привилегий, выполнить произвольный код, что может быть успешно использовано при внедрении руткита в систему. Причиной возникновения переполнения буфера или выполнения произвольного кода могут быть некорректные операции с целыми числами: явные и неявные приведения типов, в результате которых объект или выражение целого типа преобразуется к новому целому типу с диапазоном, не включающим значение объекта или выражения; арифметические операции, результат выполнения которых выходит за границы диапазона типа или имеет неопределенное значение.

В процессе внедрения руткитов эксплуатируются уязвимости, связанные с операциями чтения неопределенного значения, т. е. чтения объекта, значение которого не инициализировано либо недопустимо для типа данного объекта. Данный тип уязвимостей может использоваться для повышения привилегий или выполнения произвольного кода. Для внедрения руткитов могут использоваться уязвимости, связанные с отсутствием или некорректной проверкой входных данных (например, межсайтовый скриптинг (Cross-site Scripting)), которые позволяют нарушителю управлять выполнением кода или потоками данных приложения. В этом случае злоумышленник имеет возможность сформировать входные данные, которые будут неверно обработаны приложением, что позволит выполнить произвольный вредоносный код или подменить данные приложения [10]. Так же эксплуатируются уязвимости, связанные с некорректной обработкой данных или структур данных компонентом программного обеспечения, которые передаются на вход другого компонента программного обеспечения. Это может привести к некорректной интерпретации получаемых данных нижестоящим компонентом программного обеспечения. Данный принцип используется при реализации SQL-инъекций, XML-инъекций и т. п. [10].

Итак, для внедрения руткитов обычно используются следующие классы уязвимостей программного обеспечения:

- уязвимости, вызывающие переполнение буфера;
- уязвимости, связанные с операциями чтения неопределенного значения;
- уязвимости внесения некорректных входных данных;
- уязвимости, связанные с некорректной обработкой данных компонентом программного обеспечения при их передаче на вход другого компонента программного обеспечения.

В ходе проведенных исследований были выявлены основные характерные особенности возникновения и реализации угроз БИ, связанных с применением скрытых в операционной системе вредоносных компьютерных программ (руткитов). Результаты исследований представлены в виде комплексного описания основных возможных угроз БИ, связанных с применением скрытых

в операционной системе вредоносных компьютерных программ (руткитов). Выявление актуальных угроз БИ проводилось с помощью методов обобщения и систематизации результатов, полученных в ходе выполнения анализа основных эксплуатируемых при реализации угроз уязвимостей, основных типов источников угроз, основных возможных способов реализации угроз, основных возможных последствий угроз. Перечень и описание выявленных основных угроз БИ, связанных с применением скрытых в операционной системе вредоносных компьютерных программ (руткитов) представлены далее по тексту в таблице 1.

Угроза-1: *Внедрение в информационную систему при осуществлении информационного взаимодействия с внешними информационно-телекоммуникационными сетями скрытых вредоносных компьютерных программ.*

Аннотация угрозы: внедрение в информационную систему при осуществлении информационного взаимодействия с внешними информационно-телекоммуникационными сетями, в том числе сетями международного информационного обмена (сетями связи общего пользования), скрытых вредоносных компьютерных программ, предназначенных для: сокрытия своего присутствия в информационной системе; сокрытия присутствия другого вредоносного программного обеспечения (компьютерных вирусов) в информационной системе; сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы.

Источник угрозы: Внутренний нарушитель, внешний нарушитель.

Способ реализации угрозы: внедрение в информационную систему скрытых в операционной системе вредоносных компьютерных программ при осуществлении информационного обмена (использование механизма электронных почтовых сообщений, распространение совместно с программным обеспечением или компонентами программного обеспечения, распространение через вредоносные, взломанные или скомпрометированные веб-ресурсы).

Используемые уязвимости: неполнота комплекса средств защиты информации, применяемых в ИС.

Вид информационных ресурсов, потенциально подверженных угрозе: информационные ресурсы информационной системы, программное обеспечение информационной системы.

Нарушаемые свойства безопасности информационных ресурсов: конфиденциальность, целостность, доступность.

Возможные последствия реализации угрозы: установка на программно-технические средства информационной системы скрытых в операционной системе вредоносных компьютерных программ, функционирование скрытых в операционной системе вредоносных компьютерных программ, скрытое функционирование компьютерных вирусов на программно-технических средствах вычислительной сети информационной системы, утечка конфиденциальной информации, нарушение режимов функционирования информационной системы.

Угроза-2: *Внедрение со съемных машинных носителей информации скрытых вредоносных компьютерных программ.*

Аннотация угрозы: внедрение со съемных машинных носителей информации скрытых вредоносных компьютерных программ, предназначенных для: сокрытия своего присутствия в информационной системе; сокрытия присутствия другого вредоносного программного обеспечения (компьютерных вирусов) в информационной системе; сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы.

Источник угрозы: внутренний нарушитель.

Способ реализации угрозы: внедрение скрытых в операционной системе вредоносных компьютерных программ в информационную систему со съемных машинных носителей информации.

Используемые уязвимости: неполнота комплекса средств защиты информации, применяемых в информационной системе.

Вид информационных ресурсов, потенциально подверженных угрозе: информационные ресурсы информационной системы, программное обеспечение информационной системы.

Нарушаемые свойства безопасности информационных ресурсов: конфиденциальность, целостность, доступность.

Возможные последствия реализации угрозы: установка на программно-технические средства информационной системы скрытых в операционной системе вредоносных компьютерных программ, функционирование скрытых в операционной системе вредоносных компьютерных программ, скрытое функционирование компьютерных вирусов на программно-технических средствах вычислительной сети информационной системы, утечка конфиденциальной информации, нарушение режимов функционирования информационной системы.

Угроза-3: *Функционирование в информационной системе скрытых вредоносных компьютерных программ.*

Аннотация угрозы: функционирование в информационной системе скрытых вредоносных компьютерных программ, предназначенных для: сокрытия своего присутствия в информационной системе; сокрытия присутствия другого вредоносного программного обеспечения (компьютерных вирусов) в информационной системе; сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы.

Источник угрозы: внутренний нарушитель, внешний нарушитель.

Способ реализации угрозы: внедрение и запуск в информационной системе скрытых вредоносных компьютерных программ с использованием различных методов.

Используемые уязвимости: неполнота комплекса средств защиты информации, применяемых в информационной системе.

Вид информационных ресурсов, потенциально подверженных угрозе: информационные ресурсы информационной системы, программное обеспечение информационной системы

Нарушаемые свойства безопасности информационных ресурсов: конфиденциальность, целостность, доступность.

Возможные последствия реализации угрозы: скрытый несанкционированный доступ к информационным ресурсам информационной системы, сокрытие фактов заражения компьютерными вирусами программно-технических средств информационной системы, утечка конфиденциальной информации, нарушение режимов функционирования информационной системы.

Полученный в ходе исследования перечень угроз БИ, связанных с применением скрытых в операционной системе вредоносных компьютерных программ (руткитов), может использоваться при формировании ФТБ для средств антивирусной защиты.

Литература:

1. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации. // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2012. Спецвыпуск №5 “Информатика и системы управления”. С. 272-278.
2. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под ред. А.С. Маркова. М.:Радио и связь, 2012. 192 с.
3. Arnold T. A Comparative Analysis Of Rootkit Detection Techniques // Computer Science and Engeneering. 2011. pp. 8-16 .
4. Binsalleeh H, Ormerod T. On the Analysis of the Zeus Botnet Crimeware Toolkit // IEEE Press. 2010. pp. 4-13.
5. Каманин М.А., Браташ В.В. Применение руткит-технологий в защите данных пользователя // Информационное противодействие угрозам терроризма. 2010. № 14. С. 50-53.
6. Лагутина А.М., Богданович А.А., Иванов М.А. Руткиты. методы обнаружения и удаления // Вестник Национального исследовательского ядерного университета МИФИ. 2012. Т. 1. № 2. С. 236.
7. Лазарев Е.В., Милушков В.И. Исследование угроз информационного воздействия на антивирусы, атакуемых посредством руткит // Наука и бизнес: пути развития. 2012. № 1. С. 49-53.
8. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1 (1). С. 28-36.
9. Музыченко Я.А. Невидимость руткитов уровня ядра для средств аудита ос Linux // Вестник Российского государственного гуманитарного университета. 2009. № 10. С. 85-97.
10. Florio E. When MalwareMeets Rootkits // White Paper: Symantec Security Response. 2005. P. 22-29.
11. Костогрызов А.И., Лазарев В.М., Любимов А.Е. Прогнозирование рисков для обеспечения эффективности информационной безопасности в их жизненном цикле // Правовая информатика. 2013. № 4. С. 4-16

References:

1. Barabanov A.V., Markov A.S., Tsirlov V.L. Sertifikatsiya sredstv antivirusnoy zashchity po novym trebovaniyam bezopasnosti informatsii, Vestnik MGTU im. N.E. Baumana. Ser. «Priborostroenie», 2012, Spetsvypusk №5 “Informatika i sistemy upravleniya”, pp.272-278.
2. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviya sredstv zashchity informatsii / By ed. A.S. Markov. M.: Radio i svyaz’, 2012, 192 p.
3. Arnold T. A Comparative Analysis Of Rootkit Detection Techniques, Computer Science and Engeneering, 2011, pp. 8-16 .
4. Binsalleeh H, Ormerod T. On the Analysis of the Zeus Botnet Crimeware Toolkit, IEEE Press, 2010, pp. 4-13.
5. Kamanin M.A., Bratash V.V. Primenenie rutkit-tekhnologiy v zashchite dannykh pol’zovatelya, Informatsionnoe protivodeystvie ugrozam terrorizma, 2010, N 14, pp. 50-53.
6. Lagutina A.M., Bogdanovich A.A., Ivanov M.A. Rutkity. metody obnaruzheniya i udaleniya, Vestnik Natsional’nogo issledovatel’skogo yadernogo universiteta MIFI, 2012. V. 1, N 2, pp. 236.
7. Lazarev E.V., Milushkov V.I. Issledovanie ugroz informatsionnogo vozdeystviya na antivirusy, atakuemykh posredstvom rutkit, Nauka i biznes: puti razvitiya, 2012, N 1, pp. 49-53.
8. Markov A.S., Fadin A.A. Organizatsionno-tekhnicheskie problemy zashchity ot tselevykh vredonosnykh programm tipa Stuxnet, Voprosy kiberbezopasnosti, 2013, N 1 (1), pp. 28-36.
9. Muzychenko Ya.A. Nevidimost’ rutkitov urovnya yadra dlya sredstv audita os Linux, Vestnik Rossiyskogo gosudarstvennogo gumanitarnogo universiteta, 2009, N 10, pp. 85-97.
10. Florio E. When MalwareMeets Rootkits, White Paper: Symantec Security Response. 2005. P. 22-29.
11. Kostogry`zov A.I., Lazarev V.M., Liubimov A.E. Prognozirovanie riskov dlia obespecheniia e`ffektivnosti informatcionnoi` bezopasnosti v ikh zhiznennom tcicle // Pravovaia informatika. 2013. № 4. S. 4-16