МЕТОДИКА ОБНАРУЖЕНИЯ РУТКИТОВ, ОСНОВАННЫХ НА АППАРАТНОЙ ВИРТУАЛИЗАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Костенич Д. М.

Петровский А. А. – доцент, к.т.н.

Бурное развитие технологий аппаратной виртуализации в наши дни привлекает к себе много внимания по ряду причин. Во-первых, виртуализация предоставляет множество преимуществ, как для инфраструктуры предприятий, так и для конечных пользователей. С ее помощью обеспечивается существенная экономия на аппаратном обеспечении, обслуживании, повышается гибкость ИТ-инфраструктуры, упрощается процедура резервного копирования и восстановления после сбоев. Во-вторых, виртуальные машины, являясь независимыми от конкретного оборудования единицами, могут распространяться в качестве предустановленных шаблонов, которые могут быть запущены на любой аппаратной платформе поддерживаемой архитектуры. Однако, как показывает практика, применяться данные технологии могут не только в мирных целях. Вредоносное программное обеспечение, использующее технологии аппаратной виртуализации, может с легкостью оставаться абсолютно не обнаруживаемым для современных антивирусных программ. А с учетом того, что сегодня почти все новые x86-совместимые процессоры поддерживают аппаратную виртуализацию, руткиты, активно использующие ее, представляет серьезную угрозу. Таким образом, оценка степени опасности, исходящей от них, и разработка возможных контрмер является крайне актуальной задачей в наши дни.

Руткиты – это класс вредоносных приложений, задача которых – установить полный контроль над компьютерной системой без соответствующей процедуры авторизации. Для осуществления поставленных перед ним целей руткит должен установить в какой-либо части операционной системы свои перехватчики таким образом, что в определенный момент времени пользовательское приложение либо же сама операционная система передаст управление коду его модуля. В современных операционных системах существует множество мест, где руткиты могут разместить свои перехватчики, на основе чего строится их классификация.

Выделяют следующие категории руткитов:

- Класс 0. Руткиты данного типа заменяют существующие файлы операционной системы своими аналогами. Метод обнаружения подобных вредоносных приложений является достаточно простым, т.к. основан на сигнатурном анализе и проверке целостности системных файлов. Данный метод существует уже долгое время и внедрен практически во все антивирусное ПО.
- Класс 1. Руткиты данного типа занимаются модификацией секций кода самих исполняемых модулей операционной системы либо их таблиц импорта. Такой подход позволяет им полностью скрыть себя от приложений уровня пользователя. Метод обнаружения подобных вредоносных приложений можно построить на основе проверки целостности подписанных системных исполняемых файлов и последующем подсчете и проверке их хэш-сумм.
- Класс 2. Руткиты данного типа занимаются модификацией структур ядра операционной системы в динамике. К сожалению, универсального метода обнаружения данного типа вредоносных приложений на данный момент не существует. Проверка всех существующих структур операционной системы на целостность является слишком ресурсоемкой операцией. Поэтому текущие методы обнаружения основаны на сканировании только лишь тех структур операционной системы, которые модифицируются известными на данный момент руткитами.
- Класс 3. Руткиты данного типа являются логическим продолжением 1-го и 2-го классов. Главная их задача – захватить контроль над операционной системой, не модифицируя ее внутренних структур и логики поведения. В теории, представители этого класса должны стать «идеальными» вредоносными приложениями, которые не могут быть обнаружены. Примером данного типа вредоносного ПО является ряд концепт-руткитов (называемых также HVM-руткитами), использующих возможности аппаратной виртуализации.

Наиболее интересным представителем класса руткитов, основанных на использовании аппаратной виртуализации, является концепт-разработка с кодовым именем «Blue Pill». Первоначально программа «Blue Pill» требовала поддержки процессором виртуализации AMD-V (ранее известной как «Pacifica»), но в дальнейшем в программу была добавлена так же и поддержка Intel VT-x (кодовое имя «Vanderpool»). Разработана Йоанной Рутковской и впервые была публично продемонстрирована на конференции Black Hat Briefings 3 августа 2006 года в виде образца реализации для ядра Microsoft Windows Vista.

Концепция «Blue Pill» заключается в захвате запущенного экземпляра операционной системы (захват производится при запуске ОС) «тонким» гипервизором и виртуализацией им остальной части компьютера. Предыдущая операционная система будет все еще поддерживать существующие в ней ссылки на все устройства и файлы, но почти все, включая аппаратные прерывания, запросы данных и даже системное время будут перехватываться гипервизором, который будет отсылать фальшивые ответы.

Йоанна Рутковская утверждает, что поскольку любая программа обнаружения может быть обманута гипервизором, то такая система будет «100 % необнаруживаемой». Поскольку виртуализация от AMD была спроектирована как целостная система, то предполагается, что виртуализируемый гость не сможет опре-

делить, гость он или нет. Таким образом, единственной возможностью обнаружить «Blue Pill» является определение того факта, что виртуализированная реализация функционирует не так, как положено.

Теоретически, виртуальная машина не должна знать, что она находится в виртуальной среде. По крайней мере, на сегодняшний день не существует ни одного задокументированного способа определить это. Однако гипервизор, безусловно, будет вносить некоторые изменения в поведение виртуализируемой системы и вызывать, таким образом, различные побочные эффекты, которые можно обнаружить.

При проведении данного исследования были изучены следующие возможные методы обнаружения вредоносного гипервизора:

- Подсчет количество тактов, затраченных на выполнение специфических команд (RDMSR EFER, CPUID).
- Профилирование буферов ассоциативной трансляции.
- Классический метод анализа времени, затраченного на выполнение той или иной операции.

Полученные результаты отчетливо показывают, что разработать абсолютно необнаруживаемый руткит на текущий момент не представляется возможным. Любая технология скрытия присутствия вредоносного приложения будет оставлять следы в том или ином месте компьютерной системы, которые можно обнаружить с помощью правильных инструментов анализа.

Все вышеперечисленные методы обнаружения гипервизора были реализованы в виде драйвера с использованием WDK-пакета и протестированы в среде операционной системы Windows 7. В качестве вредоносного гипервизора выступал вышеупомянутый концепт-руткит «Blue Pill».

Основной сложностью при проведении исследования стал поиск «узких» мест функционирования гипервизора, по которым его можно обнаружить. Для решения возникшей проблемы были подробно проанализированы алгоритмы работы концепт-руткита «Blue Pill» и изучены его исходные коды.

Таким образом, был разработан и реализован ряд методов обнаружения вредоносных гипервизоров. Полученные результаты показывают, что данные методы позволяют определять наличие виртуализированной среды, а также позволяют выбрать наиболее подходящий для текущих условий метод.

Список использованных источников:

1. Они, У. Использование Microsoft Windows Driver Model / У. Они. 2-ое издание. – СПб. : Питер, 2007. – 763 с.
2. Руссинович, М. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP, Windows 2000. Мастер-класс / М. Руссинович, Д. Соломон. – СПб. : Питер, 2008. – 992 с.
3. Хогланд, Г. Руткиты. Внедрение в ядро Windows / Г. Хогланд, Дж. Батлер. – СПб. : Питер, 2007. – 283 с.