Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:004.42

Козловский
Михаил Михайлович

Методы защиты тестовых стендов от вредоносного программного обеспечения

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Шпак Иван Ильич
кандидат технических наук, доцент

_____

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

Обоснование актуальности темы магистерской диссертации. Одной из важнейших задач компьютерной безопасности является борьба с ВПО и в частности подзадача его обнаружения. В свете текущих тенденций развития вредоносных программ, все более актуальной становится задача создания эффективного средства обнаружения неизвестного ВПО.

Существующая классификация методик обнаружения ВПО включает поведенческий анализ, который, как правило, реализуется с использованием тестовых стендов, на которых происходит наблюдение за процессом выполнения исследуемых программ. В свою очередь для организации работы тестовых стендов используется виртуальная среда, поскольку по завершению анализа целевой программы данная среда может быть уничтожена без какого-либо риска для аппаратно-программной системы, обеспечивающей ее работу.

С тех пор, как эта методика получила распространение, ВПО стало включать механизмы противодействия, заключающиеся в произведении атаки на тестовый стенд или виртуальную среду, организующую его работу. В связи с этим защита тестовых стендов от подобного противодействия представляет собой **актуальную задачу**.

Оценка современного состояния решаемой задачи. В случае с использованием виртуальных сред выполнения программ, для эффективного разделения ресурсов аппаратно-программных систем в среду вносятся изменения, которые могут быть использованы ВПО с целью установления факта их запуска в виртуальной среде, а также в качестве вектора атаки на аппаратно-программную систему в целом. Для уменьшения значимости данного вектора применяется ряд подходов, позволяющих препятствовать возможности эксплуатации данных изменений, однако эти подходы ограниченны и неорганизованны.

Задачи и назначение работы. Данная работа ставит своей целью анализ вносимых изменений и возможностей их эксплуатации ВПО с целью создания эффективного программного средства для комплексного подавления значимости данного вектора атаки и улучшения защищенности тестовых стендов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований. Целью исследования является анализ векторов, используемых ВПО для атаки на тестовые стенды или компоненты их составляющие, и создание программного средства, позволяющего проводить проверку защищенности тестовых стендов от реализации данных векторов. Учитывая, что количество векторов крайне велико, это является достаточно сложной задачей.

Для достижения поставленной цели в рамках данной диссертации **были решены следующие задачи**:

- проведен анализ актуальных методов организации работы тестовых стендов;
- проведен анализ актуальных методов противодействия запуску на тестовых стендах;
- разработаны методы парирования противодействия запуску на тестовых стендах;
- разработано и отлажено программное средство для проверки защищенности тестовых стендов от воздействия ВПО.

Теоретическая и практическая значимость. Теоретическая значимость работы заключается в разработанных методах защиты тестовых стендов от воздействия ВПО, а также программном средстве для проверки защищенности тестовых стендов от воздействия ВПО. Практическая ценность работы заключается во внедрении результатов исследования в учебный процесс в 2014-2015 учебном году в лекционном курсе по дисциплине «Основы защиты информации и управления интеллектуальной собственностью» в виде лекционного материала для студентов заочной формы обучения по специальности 1-39 02 01 Моделирование и компьютерное проектирование радиоэлектронных средств, а также использовании результатов в ходе трудовой деятельности в ООО «Группа информационно безопасности» г. Москва, Российская федерация.

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом по месту трудовой деятельности в ООО «Группа информационной безопасности», г. Москва, Российская Федерация.

Результаты работы опубликованы в:

– Козловский М.М., Шпак И.И. Анализ уязвимостей виртуальных сред выполнения программ // // Современные средства связи: материалы XVIII

Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 229-230.

– Козловский М. М. Исследование уязвимостей эмуляции отладочных возможностей процессора в мониторах виртуальных машин // 50-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014. – 78 с. с ил. – С. 45

– Козловский М.М., Шпак И.И. Анализ уязвимостей эмуляции отладочных возможностей процессора в мониторах виртуальных машин // Материалы XX МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014. – С. 265

– Козловский М.М., Козлов К.С. Алгоритм расследования инцидентов в электромобилях, вызванных вредоносным программным обеспечением // Современные тенденции развития науки и производства: сборник материалов Международной научно-практической конференции (23-24 октября 2014 года), в 4-х томах. – Том 1. – Кемерово: ООО «ЗапСибНЦ», 2014 – 196 с. – С. 37-39

Результаты работы апробированы на 4 (четырех) научно-технических конференциях, в том числе 3 (трех) международных:

– XVIII Междунар. науч.-техн. конф. «Современные средства связи», 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.].

– XX МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014

– 50-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014

– МНТК «Современные тенденции развития науки и производства», Кемерово (23-24 октября 2014 г.) – Кемерово: ООО «ЗапСибНЦ», 2014

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из введения, общей характеристики работы, трех глав, заключения и двух приложений.

В первой главе «Краткая классификация ВПО» рассмотрены основные угрозы информационной безопасности и дано определение объекта исследования. Рассмотрены основные виды вредоносного программного обеспечения, а также основные предпосылки к возникновению угроз информационной безопасности.

Во второй главе «Теоретические основы анализа вредоносных файлов» рассмотрены методология анализа с точки зрения криминалистического исследования. Проведен эксперимент по анализы вредоносного файлы, в результате которого был получен набор его функциональных возможностей. Указаны предпосылки к использованию объекта исследования в целях упрощения анализы.

В третьей главе «Виртуальные среды выполнения программ и их угрозы» дана краткая классификация виртуальных машины, организующих работу виртуальных сред выполнения программ и объекта исследования в частности. Рассмотрены основные виды угроз с точки зрения модели использовании, в которой основным пользователем выступает аналитик-криминалист. Также предложены методы парирования данных угроз и сделаны выводы.

Код программного средства для проверки защищенности тестовых стендов от вышеуказанных угроз приведен в первом приложении.

ЗАКЛЮЧЕНИЕ

• Проведен анализ актуальных методов организации работы тестовых стендов. Выяснено следующее:

– использование виртуальных сред выполнения программ в качестве основы для организации работы тестового стенда является крайне разумным шагом;

– анализ образцов ВПО с использованием статическим методов является крайне трудоемким процессом;

– использование динамических методов, в частности системного монитора, работающего на основе виртуальной среды, может значительно сократить накладные расходы специалиста на анализ;

– механизмы ВПО, препятствующие запуску в виртуальной среде не позволяют в полной мере воспользоваться динамическими методами анализа.

• Проведен анализ актуальных методов противодействия запуску на тестовых стендах и разработаны методы парирования противодействия запуску на тестовых стендах. Сделаны следующие выводы:

– угрозы информационной безопасности «атака на отказ в обслуживании» и «побег из виртуального окружения» могут быть реализованы только при реализации угрозы «обнаружение выполнения в виртуальной среде»;

– не существует эффективных мер подавления угроз «атака на отказ в обслуживании» и «побег из виртуального окружения», кроме контроля качества реализации компонентов виртуальной машины и сведения к минимуму взаимодействие ведущей и ведомой операционных систем;

– обнаружение выполнения в виртуальной среде может быть парировано путем использования собственной реализации гипервизора, который не должен общаться с ведомой гостевой системой, однако должен поддерживать работоспособность и скрытность системного монитора, выполняющегося под его управлением.

• Разработано и отлажено программное средство для проверки защищенности тестовых стендов от воздействия ВПО.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

[1-А] Козловский М.М., Шпак И.И. Анализ уязвимостей виртуальных сред выполнения программ // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 229-230.

[2-А] Козловский М. М. Исследование уязвимостей эмуляции отладочных возможностей процессора в мониторах виртуальных машин // 50-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014. – 78 с. с ил. – С. 45

[3-А] Козловский М.М., Шпак И.И. Анализ уязвимостей эмуляции отладочных возможностей процессора в мониторах виртуальных машин // Материалы XX МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014. – С. 265

[4-А] Козловский М.М., Козлов К.С. Алгоритм расследования инцидентов в электромобилях, вызванных вредоносным программным обеспечением // Современные тенденции развития науки и производства: сборник материалов Международной научно-практической конференции (23-24 октября 2014 года), в 4-х томах. – Том 1. – Кемерово: ООО «ЗапСибНЦ», 2014 – 196 с. – С. 37-39.