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

УДК 004.056+004.491

Пушнов
Юрий Александрович

Анализ методов обфускации программных средств и оценка их эффективности

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик В.Н.
д.т.н., профессор

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

Большое количество вредоносных файлов, которые ежедневно выпускаются, превосходит текущие возможности анализа и их обнаружения. Например, Intel Security Labs сообщает, что в течение каждого часа в третьем квартале 2015 года более 3,5 миллионов зараженных файлов были обнаружены в пользовательских сетях, кроме того было выявлено 7,4 миллиона попыток установки или запуска потенциально нежелательного ПО. Ущерб, наносимый вредоносными атаками, также становится все более разрушительным, о чем свидетельствует недавний вредоносный код Cryptowall, который, как сообщается, привел к выплате в 325 миллионов долларов выкупа преступникам.

В настоящее время вредоносное ПО используется в широком спектре атак, от распространения по сети, а также от атак типа «отказ в обслуживании» (DoS) на веб-серверы, что приводит к сбоям в обслуживании и краже информации о кредитных карточках для более сложных атак на атомные станции. Кроме того, количество вредоносных программ увеличивается, и каждый год их влияние возрастает. Например, вредоносные программы Carbanak смогли украсть $ 1 млрд из более чем 100 финансовых учреждений по всему миру в крупнейшей банковской истории в истории [20].

Каждый год выпускается и распространяется огромное количество вредоносных программ, и производители антивирусных программ изо всех сил стараются не отставать, работая над своевременным обновлением своих приложений для клиентов. В последнем квартале 2014 года McAfee получил более 350 миллионов образцов вредоносного ПО, из которых 50 миллионов были новыми вредоносными программами. Это означает, что каждую минуту появляется 387 новых угроз.

Несмотря на разнообразие средств защиты от вредоносных программ, от хоста до сетевых решений, обнаружение вредоносных программ остается открытой проблемой. Основным усложнением решения проблемы является то, что атаки вредоносного ПО постоянно меняются. Вредоносные программы используют несколько методов, чтобы избежать обнаружения и быстро эволюционировать по сравнению с решениями обнаружения. Существуют методы, которые ускользают от обнаружения сигнатур, такие как простое шифрование, полиморфизм или продвинутый метаморфизм. Другие методы нацеливают анализ поведения через обнаружение виртуальной машины, или даже используют мимические атаки, чтобы обмануть систему поведенческого анализа, показав доброкачественное поведение.

Одним из основных методов сокрытия исходного кода программы является метод обфускации. Существуют различные методы обфускации, которые могут быть одновременно применены к исполняемому коду программного средства. Эти методы постоянно совершенствуются и обновляются. По этой причине для эффективной защиты от вредоносных ПС необходимы новые методики. Также необходимо разработать новые или усовершенствовать существующие методы автоматического обнаружения вредоносного ПО, которые одновременно производили деобфускацию программ с различной степенью запутанности кода.

В данной работе будут описаны типы вредоносных программ, методы, используемые для их защиты от анализа, а также методы для обнаружения небезопасного программного обеспечения.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель магистерской диссертации – провести исследование существующих методов обфускации и их использование для защиты вредоносного ПО от обнаружения; выяснить и предложить улучшения к существующим методам анализа запутанного исходного кода; проработать достигнутые в области анализа обфусцированных программ результаты; предложить оценку возможности использования описанных методов.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести исследование существующих типов вредоносного ПО.
2. Выявить основные способы запутывания исходного кода программы.
3. Провести исследование различных методов обфускации программного кода.
4. Определить методы автоматического исследования запутанного кода.
5. Предложить улучшения к существующим методам и метрикам анализа.

Объектом магистерской диссертации являются методы и способы защиты программного обеспечения с помощью методов обфускации.

Предметом магистерской диссертации является нахождение эффективных методов исследования обфусцированного кода на примере вредоносного ПО. Основная *гипотеза*, положенная в основу работы: большинство современных вредоносных программ используют существующие методы обфускации, их комбинации и модификации; авторы вредоносного ПО постоянно обновляют способы запутывания исходного кода программы. Особенностью исследуемой темы является то, что среди методов запутывания исходного кода того или иного программного средства, наблюдаются небольшие отличия в использовании методов обфускации. Однако для эффективного обнаружения вредоносного ПО требуется автоматизация процесса деобфускации и обнаружения злонамерного поведения. Таким образом экспериментальное исследование становится невозможным без программных компонентов, исследование и описание работы которых является неотъемлемой частью данной работы.

Связь работы с приоритетными направлениями научных исследовний и запросами реального сектора экономики

1. Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Разработка моделей, методов, алгоритмов, повышающих показте-

ли проектирования, внедрения и эксплуатации программных средств для адач, работы с большими массивами данных и внедрение в современные обучающие комплексы» (ГБ No 16-2004, No ГР 20163588, научный руководитель НИР – Н. В. Лапицкая).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя В. Н. Ярмолика, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на XXII Республиканский конкурса научных работ студентов (2015 год).

Опубликованность результатов диссертации

По теме диссертации опубликована 1 печатная работа в сборниках трудов и материалов международных конференций.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и пяти приложений. В главе 1 приводится исследование типов вредоносных систем и способы сокрытия их исходного кода. Глава 2 посвящена исследованию существующих методов обфускации, которые применяются к исходному коду программных средств. В главе 3 анализируются методы анализа и поиска обфусцированного вредоносного ПО.

Общий объем работы составляет 54 страницы, из которых основного текста – 46 страниц, 8 рисунков на 7 страницах, 5 таблицы на 4 страницах, список использованных источников из 21 наименование на 2 страницах и 1 приложение на 1 странице.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В **первой главе** проведен анализ существующих типов вредоносного ПО, их основные характеристики, а также методы защиты программного кода от анализа.

Вредоносная программа – это общий термин, используемый для обозначения различных форм враждебного или навязчивого программного обеспечения, включая компьютерные вирусы, черви, трояны, вымогатель, шпионское ПО, рекламное ПО и другие вредоносные программы. Он может принимать форму исполняемого кода, скриптов, активного содержимого и другого программного обеспечения. Вредоносные программы часто замаскированы как вредоносные файлы или внедрены в них. По состоянию на 2011 год большинство активных угроз вредоносных программ были червями или троянами, а не вирусами.

Шпионское ПО или другое вредоносное ПО иногда обнаруживается в программах, официально предоставляемых компаниями, например, загружаемых с веб-сайтов, которые кажутся полезными или привлекательными, но могут иметь, например, дополнительные скрытые функции отслеживания, которые собирают статистику маркетинга. Примером такого программного обеспечения, которое было охарактеризовано как незаконное, является руткит Sony, троян, встроенный в компакт-диски, продаваемые Sony, которые молча устанавливали и скрывали себя на компьютерах покупателей с целью предотвращения незаконного копирования; Он также сообщил о привычках слушателей к прослушиванию и непреднамеренно созданных уязвимостях, которые использовались несвязанными вредоносными программами.

Такие программы, как антивирус и брандмауэры, используются для защиты от активности, обозначенной как вредоносная, и для восстановления после атак.

Вторая глава посвящена описанию обфускации как методу программной защиты программного обеспечения.

Были описаны различные методы обфускации. Также для некоторых были приведены примеры реализаций на современных языках программирования.

Суть процесса обфускации заключается в том, чтобы запутать программный код и устранить большинство логических связей в нем, то есть трансформировать его так, чтобы он был очень труден для изучения и модификации посторонними лицами (будь то взломщики, или программисты, которые собираются узнать уникальный алгоритм работы защищаемой программы).

Обфускация соответствует принципу экономической целесообразности, так как ее использование не сильно увеличивает стоимость программного продукта и позволяет при этом снизить потери от пиратства и уменьшить возможность плагиата в результате кражи уникального алгоритма работы защищаемого программного продукта.

В **третьей главе** представляет методы обнаружения вредоносного ПО, а также анализа исходного кода вредоносных программ.

Более детально проанализированы возможности исследования программ на наличие скрытых инструкции. Основой исследования являлся граф потока управления программ.

Использование данного метода позволяет упрощать процесс обнаружения вредоносного ПО. Также оно включает возможность совершенствования описанных методов, в том числе с помощью нейронных сетей и других средств автоматизации и самообучения. [1]

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведено описание и исследование поведения разновидностей вредоносного ПО.

2. Перечислены методы, применяемые для детального анализа изучения поведения вредоносных средств. Описаны их достоинства их недостатки.

3. Обобщены и описаны итоги применения методов обфускации исходного кода программных средств. Описаны их характеристики и дана оценка степени их эффективности.

4. Изучены основные методы противодействия исследованию программного кода вредоносного ПО.

5. Предложен метод исследования обфусцированного кода вредоносного ПО, основанный на изучении графа потока управления программы.

6. Выполнено сравнение применения описанных методов как для злонамеренного программного обеспечения, так и для файлов, не предоставляющих угрозу для пользователя.

7. Обобщены и описаны итоги применения методов выявления вредоносного ПО. Выделены достоинства и недостатки.

8. Обозначены возможные улучшения описанных методов, которые могут быть разработаны для более быстрого и качественного анализа программных средств.

Рекомендации по практическому использованию результатов

1. Полученные результаты формируют теоретическую и практическую базу для анализа обфусцированного вредоносного ПО.

2. Предложена модель оценки обфусцированного ПО на наличие вредоносного поведения может быть использована для долгосрочного процесса выявления вредоносных программ.

3. Результаты могут использоваться изучения поведения вредоносного ПО, а также как база для дальнейшего усовершенствования и применения описанных методов для исследования программных средств.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Пушнов, Ю. А. Защита программного обеспечения с помощью методов обфускации / Ю. А. Пушнов // XXII Республиканский конкурса научных работ студентов. – Минск, 2015.