УДК 004.492.3

ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ ЗАЩИТЫ ОТ МАКРОВИРУСОВ

Нестеров Д.К. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Маркина Т.А.
(Университет ИТМО)

В работе рассмотрены способы обфускации макровирусов, которые позволяют им оставаться незамеченными для антивирусного программного обеспечения, а также описано разработанное решение для обнаружения таких макровирусов.

Введение. Макровирусы – это разновидность компьютерных вирусов, написанных на макроязыках и встраиваемых в различное прикладное программное обеспечение.

В качестве примера можно привести штамм макровирусов Emotet. Он распространялся по почте маскируясь под различные подлинные документы (например, накладные и резюме) так, что их получатель, ничего не подозревая, открывал зараженный файл.

Современное антивирусное ПО способно обнаруживать большое количество макровирусов. Для обеспечения наибольшей точности можно использовать VirusTotal – вебсайт, который позволяет проверить файл на вирусы с использованием более чем 60 популярных антивирусных программ.

Однако, обширные возможности макроязыков и плохо задокументированные проприетарные форматы файлов от Microsoft до сих пор позволяют злоумышленникам создавать макровирусы, которые остаются необнаруженными ни одним или очень малым числом антивирусного ПО.

Одним из лучших решений в данной области является oletools – сборник инструментов, запускаемых из командной строки, для анализа исходного кода макросов, встроенных в документы Microsoft Office. Эти инструменты, однако, неудобны для рядового пользователя и неспособны автоматически анализировать новые файлы для своевременного предупреждения пользователей.

Основная часть. Популярными методами защиты от вирусов являются методы сканирования сигнатур и методы отслеживания поведения программ. Однако, это не очень эффективные меры против макровирусов, поскольку их можно легко обфусцировать, избегая попадания под сигнатуру, а при обнаружении слежки они могут менять свое поведение.

Оптимальным методом в обнаружении макровирусов является статический анализ их исходного кода. Предлагаемым решением является веб-приложение, которое осуществляет поиск макросов в файлах пакета Microsoft Office и находит в них ключевые операции, которые могут взаимодействовать с файловой системой или исполнять программы, а также ключевые слова, соответствующие автоматическому исполнению кода при открытии/закрытии документа. После этого программа выдает вердикт о том, является ли загруженный файл вредоносным.

Специализация приложения на макровирусах делает его полезным в том числе и для аналитиков благодаря просмотру исходного кода и списка опасных операций, а также различным возможностям по деобфускации кода.

Основным преимуществом представленного решения перед oletools является наличие графического интерфейса и отсутствие необходимости в установке приложения, что делает его удобным в использовании для рядового пользователя.

Представленное приложение позволяет обнаруживать больше макровирусов, чем VirusTotal, поскольку оно полагается не только на исходный код макросов, но и на скомпилированную версию кода, называемую *p-code*.

Выводы. Полученный опыт можно применить в разработке антивирусного ПО для увеличения уровня защиты от макровирусов.

Также для постоянной защиты пользователей разработанную программу можно оформить в виде расширения для браузера, которое автоматически анализирует скачиваемые файлы и предупреждает пользователя в случае обнаружения макровирусов.

Нестеров Д.К. (автор) Подпись

Маркина Т.А. (научный руководитель) Подпись