МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Сбор и анализ информации об EXE-файлах на основе открытых источников

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Енца Михаила Владимировича

Научный руководитель
доцент _____ И. Ю. Юрин
23.01.2020 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2020 г.

Саратов 2020

ВВЕДЕНИЕ

При исследовании вредоносных программ формата PE (Portable Executable) довольно часто необходима информация об обстоятельствах создания файла. Бывает полезным выяснить первоначальное имя файла, потому что большинство программистов предпочитают давать своим программам имена, однозначно определяющие их назначение. Адрес сетевого ресурса, к которому обращается файл в процессе своей работы, является важным звеном при анализе поведения исполняемого файла. Также к такой информации можно отнести название использованного при создании файла компилятора, дату и время компиляции, манифест файла и многое другое. Все это часто вкладывается в файл самим компилятором. Подобная информация позволяет составить поведенческий портрет автора и найти связи между различными цифровыми файлами, что в итоге может привести к однозначной идентификации создателя файла или группы файлов.

Существует довольно много программ-анализаторов PE-файлов. Анализаторы PE-файла действительно предоставляют требуемую информацию, например, версию использованного при создании файла компоновщика, но если не знать, что в PE-файле эта информация хранится в Optional Header, то поиск в программе может занять некоторое время.

Целями данной работы являются:

- Изучение внутреннего строения PE-файлов;
- Исследование работа существующих анализаторов этих файлов;
- Разработка собственной программы для автоматического извлечения криминалистически значимой информации из исполняемых файлов;
- Интеграция функционала разработанной программы в программу для поиска на основе открытых источников Maltego.

Дипломная работа состоит из введения, 7 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 104

страницы, из них 67 страниц – основное содержание, включая 36 рисунков и 15 таблиц, список использованных источников из 15 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе подробно рассматривается внутренняя структура формата PE. Описание секций, важных смещений и размеров полей в структурах секций. Эти данные необходимы для понимания того, как и где могут располагаться чувствительные данные.

Во втором разделе работы описываются статические данные, которые можно извлечь из PE-файла. Такие данные представляют интерес и являются отправной точкой при составлении карты зависимостей между структурными элементами внутри файла, а также зависимостей между другими файлами.

Подраздел 2.1 содержит описание упаковщиков и программ защиты. Приводится описание принципов работы и следов, которые остаются в файле в результате работы таких программ.

Подраздел 2.2 содержит описание понятия сигнатуры, распространённые виды сигнатур и средства для автоматического детектирования сигнатур в файлах. Также приводится пример способа расшифровки сигнатуры «Rich».

В подразделе 2.3 описывается содержание секции ресурсов в исполняемом файле, а также раздел в PE-файле VS_VERSIONINFO.

В подразделе 2.4 содержится описание манифеста исполняемого файла.

Информация об оверлее, местах его расположения и информация, которую можно из него извлечь, содержится в разделе 2.5.

Цифровая подпись файла описывается в подразделе 2.6.

Подраздел 2.7 содержит информацию о списке использованных функций в исполняемом файле. Также приводится краткое описание часто используемых динамических библиотек.

Информацию о строковых данных, которые можно извлечь из исполнимого файла, содержится в подразделе 2.8.

В третьем разделе описываются аномалии, которые можно найти в PE-файле. Аномалии являются сильным критерием при классификации файлов по происхождения и поведению. Несоответствие структуре формата PE является

важнейшим моментом при анализе. При нахождении расхождения можно утверждать, что файл был модифицирован каким-то образом: либо в автоматическом режиме, либо в ручном. В разделе приводятся распространенные аномалии, относящиеся к различным сегментам PE-файла.

В четвертом разделе производится обзор и сравнение программ-анализаторов PE-файлов. Приводятся плюсы, минусы и функциональные различия между программами. Рассматриваются такие программы как: «PE Explorer», «CFF Explorer», «FileAlyzer», «PEiD».

В пятом разделе содержится описание принципов поиска и анализа вредоносных файлов с помощью открытых источников. Раздел содержит рекомендации для безопасного сбора данных в сети Интернет.

В шестом разделе содержится описание программы Maltego, сравнение версий релизов программы, описание интерфейса и примеры работы. Программа Maltego является очень удобным инструментом при построении зависимостей, а автоматический режим создания связей делает этот инструмент интересным для исследователей при анализе путей распространения угроз.

Седьмой раздел содержит описание архитектуры и возможностей разработанной программы. Программа позволяет находить соответствия между различными сущностями. Большая часть сущностей может быть извлечена из исполняемых файлов. Таким образом можно находить файлы, которые имеют общие части, также можно категорировать их по направленности их применения и авторству.

Подраздел 7.1 содержит описание разработанной программы вместе с примерами результатов работы.

В подразделе 7.2 описывается пошаговый пример работы программы при исследовании набора вредоносных файлов.

Способ интеграции и пример взаимодействия разработанной программы с программой Maltego описываются в подразделе 7.3. В конечном итоге интеграция разработанной программы с Maltego обеспечила очень удобный инструмент для анализа вредоносных файлов. Этот симбиоз позволил найти

семейство вредоносных программ, которые связаны по сигнатуре пути в файловой системе и email-адресу. При дальнейшем раскрытии дочерних сущностей можно обнаружить множество неочевидных связей.

В приложениях представлены фрагменты исходного кода программы, наиболее важные классы и интерфейсы, относящиеся к логике программы. Похожие фрагменты кода, касающиеся сущностей, по возможности исключены.

ЗАКЛЮЧЕНИЕ

В ходе работы было изучено внутреннее строение PE-файлов, рассмотрено и проведено сравнение работы существующих анализаторов исполнимых файлов, также была разработана собственная программа с интеграцией функционала в программу Maltego для автоматического извлечения, анализа и сравнения криминалистически значимой информации из исполняемых файлов. Существующие программы для работы с PE-файлами отлично справляются с анализом единичных файлов, но часто экспертам необходима не только разрозненная информация о файлах, но и сравнение их между собой. Такие исследования позволяют найти зависимости, которые в конечном счете позволят создать защиту от вредоносных файлов или даже обнаружить причастность автора какого-либо вредоносного файла к другим.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Зайцев, О. В. ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. / О. В. Зайцев. – СПб.: БХВ-Петербург, 2006. – 304 с.

2 Сикорски, М. Вскрытие покажет! Практический анализ вредоносного ПО. / М. Сикорски, Э. Хониг. – СПб.: Питер, 2018. – 768 с.

3 Кормен, Т. Х. Алгоритмы: построение и анализ, 2-е издание / Т. Х. Кормен, Ч. И. Лейзернон, Р. Л. Ривест. – Издательский дом “Вильямс”, 2005. – 1296 с.

4 Касперски, К. Искусство дизассемблирования / К. Касперски, Е. Рокко. – СПб.: БХВ-Петербург, 2008. – 893 с.

5 Панов, А. С. Реверсинг и защита программ от взлома / А. С. Панов. – СПб.: БХВ-Петербург, 2006. – 256 с.

6 Касперски, К. Техника отладки программ без исходных текстов / К. Касперски. – СПб.: БХВ-Петербург, 2005. – 832 с.

7 Климентьев, К. Е. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Климентьев. – М.: ДМК Пресс, 2013. - 656 с.

8 Alvarez, V. M. Welcome to YARA’s documentation! – портал онлайн документации / V. M. Alvarez [Электронный ресурс] : [сайт]. – URL: https://yara.readthedocs.io/en/v3.4.0/index.html (дата обращения 01.10.2019). - Загл. с экрана. - Яз. Англ.

9 PE_TEKKEN.A - Threat Encyclopedia - Trend Micro RU – портал компании Trend Micro об информационной безопасности / [Электронный ресурс] : [сайт]. - URL: https://www.trendmicro.com/vinfo/ru/threat-encyclopedia/archive/malware/pe_tekken.a (дата обращения 13.11.2019). – Загл. с экрана. - Яз. Англ.

10 Szor, P. Attacks on Win32 // Virus Bulletin, 1998. – P. 57-84.

11 Szor, P. Atacks on Win32 – Part II // Virus Bulletin, 2000. – P. 47-68.

12 Tor Project | Anonymity Online / [Электронный ресурс] : [сайт]. – URL: https://www.torproject.org/ (дата обращения 15.11.2019). - Загл. с экрана. - Яз. Англ.

13 Лутц, М. Изучаем Python, 4-е издание / М. Лутц. – СПб.: Символ-Плюс, 2011. – 1280 с.

14 Maltego Classic / [Электронный ресурс] : [сайт]. – URL: https://www.paterva.com/ (дата обращения 12.10.2019). – Загл. с экрана. – Яз. Англ.

15 4 релиза Maltego. Принцип работы и возможности / [Электронный ресурс] : [сайт]. – URL: https://habr.com/ru/company/tomhunter/blog/462457/ (Дата обращения 15.12.2019). – Загл. с экрана. – Яз. Рус.