Impact Factor: 9.9 ISSN-L: 2544-980X

Компьютерные Вирусы И Вопросы Защиты От Вирусов

МЭ Санаев [1], Эльмуродова Фарида Фаридовна [2]

Абстракт: Множество определений компьютерного вируса. Первое определение было дано Фредом Коэном в 1984 году: «Компьютерный вирус-это программа, которая заражает и модифицирует другие программы, внедряя в них себя или модифицированную копию.

При этом внедренная программа сохраняет способность к воспроизведению». Способность вируса воспроизводить себя и изменять вычислительный процесс являются ключевыми понятиями в этом определении. Эти особенности компьютерного вируса аналогичны паразитизму биологических вирусов в живых организмах.

Ключевые слова: Компьютерный вирус, самовосстановление, жилое пространство, разрушительный потенциал.

Introduction

В настоящее время компьютерный вирус представляет собой программный код, имеющий следующие характеристики:

- обязательно соответствующих оригиналу, но имеющих характеристики оригинала (самовосстановление);
- наличие механизмов, обеспечивающих включение созданных копий в исполняемые объекты компьютерной системы.

Следует отметить, что эти характеристики необходимы, но недостаточны. Указанные свойства должны быть дополнены свойствами деструктивности и нераскрытия воздействия вредоносных программ в вычислительной среде.

Вирусы можно классифицировать по следующим основным признакам :

- жилое пространство;
- Операционная система;
- особенность алгоритма производительности;
- разрушительный потенциал.

Компьютерные вирусы принято классифицировать по месту их обитания, иными словами, по типам объектов компьютерной системы, в которые проникают вирусы (рис. 1.1).

Файловые вирусы внедряются в исполняемые файлы различными способами (наиболее распространенные типы вирусов): либо путем создания файлов-двойников (вирусы-компаньоны), либо путем использования способности к организации файловых систем (вирусы-ссылки).

Methodology

Скачать вирусы записывает себя в загрузочный сектор диска (boot-сектор) или в сектор, который является системным загрузчиком (MasterBootRecord) винчестера. Загрузочные вирусы действуют как программный код, который берет на себя управление при загрузке системы.

[1] Самаркандский филиал международной школы финансовых технологий и науки
[2] Самаркандский филиал международной школы финансовых технологий и науки Студент

1.1. Классификация компьютерных вирусов по среде обитания заражают макропрограммы и файлы современных систем обработки информации, в частности Microsoft Word, Microsoft Excel и др. отравляет файлы и таблицы массовых редакторов, таких как.

Сетевые вирусы использует компьютерные сети, протоколы и команды электронной почты для своего распространения. Сетевые вирусы иногда называют программами-червями. Сетевые вирусы делятся на интернет-червей (распространяющихся через Интернет) , IRC-червей (чатов, InternetRelayChat).

Множество комбинированных типов компьютерных вирусов, например сетевой макровирус заражает редактируемые документы и распространяет их копии по электронной почте. Другой пример-файловозагружающие вирусы, заражающие файлы и загрузочный сектор дисков.

Жизненный цикл вирусов. Как и любую программу, компьютерные вирусы можно разделить на две основные стадии жизненного цикла-стадии хранения и стадии выполнения.

Фаза хранения соответствует периоду хранения вируса на диске вместе с объектом, в который он был внедрен. На этом этапе вирус уязвим для антивирусного программного обеспечения, поскольку он неактивен и не может контролировать операционную систему на предмет защиты.

Цикл исполнения компьютерных вирусов обычно включает пять стадий:

1. Загрузка вируса в память.
2. Найдите жертву.
3. Отравление найденной жертвы.
4. Выполнение деструктивных функций.
5. Передача управления вирусоносителю.

Загрузите вирус в память. Вирус загружается в память операционной системой одновременно с исполняемым объектом, в который вставляется вирус. Например, если пользователь запускает программный файл, содержащий вирус, код вируса, очевидно, будет загружен в память как часть этого файла . Обычно процесс загрузки вируса заключается в его копировании с диска в оперативную память, а затем передаче управления телу кода вируса. Эти действия выполняет операционная система, сам вирус находится в пассивном состоянии. В более сложных задачах вирус после взятия управления может выполнять дополнительные действия для своей работы. Здесь есть два аспекта.

Results and discussion

связан с максимальной сложностью процедур обнаружения вирусов. На этапе хранения некоторые вирусы используют достаточно сложный алгоритм обеспечения защиты. К такой сложности может относиться шифрование основной части вируса. Но использовать только шифрование-плохое решение, поскольку часть вируса, обеспечивающая расшифровку, должна находиться на виду на этапе загрузки. Чтобы избежать подобной ситуации, разработчики вирусов используют механизм «мутации» кода дешифратора. Суть этого метода заключается в том, что при внедрении в объект копии вируса его расшифрованная часть модифицируется таким образом, что появляются текстовые различия с оригиналом , но результат работы не меняется.

Вирусы, использующие механизм мутации кода, называются *полиморфными вирусами* . Полиморфные вирусы (полиморфные)-это вирусы, которые трудно обнаружить и не имеют сигнатур, то есть не содержат какой-либо постоянной части своего кода. Полиморфизм встречается у файловых, загружаемых и макровирусов.

При использовании стелс-алгоритмов вирусы могут полностью или частично блокироваться в системе . вирусы, использующие стелс-алгоритмы, называются *стелс-вирусами (Stealth). Вирусы-невидимки* скрывают свое существование, перехватывая доступ операционной системы

к поврежденным файлам и перенаправляя операционную систему к неповрежденной части информации.

Второй аспект связан с так называемыми *резидентными вирусами*. Поскольку вирус и объект, в который он внедрен, являются для операционной системы одним целым, после загрузки они естественным образом располагаются в едином адресном пространстве. Когда объект завершен, он освобождается из оперативной памяти. При этом вирус высвобождается и переходит на пассивную стадию хранения. Но некоторые вирусы обладают способностью сохраняться в памяти и оставаться активными после того, как вирусоноситель завершил свою работу. Такие вирусы называются резидентными. Резидентные вирусы обычно отравляют жизненное пространство, используя только привилегированные режимы, разрешенные операционной системе, и при определенных условиях действуют как вредоносное ПО. Резидентные вирусы находятся в памяти и остаются активными до выключения компьютера или перезагрузки операционной системы .

Нерезидентные вирусы выполняют задачи отравления и заражения только при их активации . Затем эти вирусы полностью покидают память и остаются в жизненном пространстве.

Следует отметить, что деление вирусов на резидентные и нерезидентные относится только к файловым вирусам. Загрузчик и макровирусы относятся к резидентным вирусам.

Найдите жертву. Вирусы делятся на два класса по способу поиска жертвы . К первому классу относятся вирусы, осуществляющие активный поиск с использованием функций операционной системы. Ко второму классу относятся вирусы, реализующие механизмы пассивного поиска, то есть устанавливающие ловушки для программных файлов.

Отравление найденной жертвы. В общем, отравление означает, что код вируса копирует себя в объекте, выбранном в качестве жертвы.

рассмотрим отравляющие свойства файловых вирусов. При этом различают два класса вирусов. Вирусы первого класса не вставляют свой код непосредственно в файл программы, а меняют имя файла и создают новый файл с телом вируса. Ко второму классу относятся вирусы, проникающие непосредственно в файлы жертвы. Эти вирусы характеризуются местами проникновения. Могут быть доступны следующие варианты:

1. *Вставьте в начало файла.* Этот метод наиболее удобен для *com-файлов MS-DOS*, поскольку в этом формате предусмотрены служебные заголовки.
2. *Вставка конца файла.* Этот метод является наиболее распространенным, и передача управления коду вируса обеспечивается путем изменения первой команды программы *(com)* или заголовка файла *(exe)*.
3. *Вставьте в середину файла.* Этот метод обычно используется, когда структура вируса применяется к заранее известным файлам (например, файлу *Command.com*) или файлам, которые содержат последовательность байтов с одинаковым значением и имеют достаточную длину, чтобы содержать вирус.

Характеристики стадии заражения загрузочными вирусами определяются объектами, в которые они попадают, - качеством загрузочных секторов ленточных и жестких дисков и главной загрузочной записи (MBR) жесткого диска. Основная проблема – ограниченный размер этого объекта. Поэтому вирусы должны хранить на диске свой фрагмент, не помещающийся в местонахождении жертвы, и нести в себе исходный код зараженного загрузчика.

Для макровирусов процесс заражения заключается в сохранении кода вируса в выбранном документе-жертве . Для некоторых программ обработки данных это сделать непросто, поскольку формат файла документа может быть не предназначен для хранения макросов.

Conclusion

Выполнение деструктивных функций. По своим разрушительным возможностям вирусы классифицируются на безвредные, безопасные, опасные и очень опасные.

Вирусы – это вирусы с механизмом саморазмножения . Они не вредят системе, а просто используют свободное место на диске.

Безопасные вирусы – вирусы, связанные с различными впечатлениями (звуком, видео) в системе, уменьшая при этом свободную память, не нанося вреда программам и данным.

Опасные вирусы – вирусы, вызывающие серьезные сбои в работе компьютера. В результате программное обеспечение и данные могут быть повреждены.

Очень опасные вирусы — вирусы, которые непосредственно приводят к уничтожению программ и данных, а также к удалению необходимой для работы компьютера информации, обработка которой заложена заранее в алгоритмы обработки.

Передача управления вирусоносителю . Следует отметить, что вирусы делятся на деструктивные и недеструктивные.

Вредоносные вирусы не заботятся о сохранении функциональности программ при их заражении, поэтому этот шаг для них бессмысленен.

неразрушающих вирусов этот этап включает восстановление программы в памяти до формы, необходимой для ее корректного функционирования, и передачу управления носителю вирусной программы.

Список использованных литератур

1. Eshquvvat o’g’li M.S, Zafar qizi Z.B Areas of application of artificial intelligence issn: 2181-4027 sjif: 4.995 Volume-27, Issue-2, February-2023. 61-64.
2. Eshquvvat o’g’li M.S, Naim o‘g‘li M. D, Xamrobek o’g’li N.N, Data miningda crisp-dm metodoligiyasi tasnifi Часть-11_ Том-1_ Декабрь-2023 43-46.
3. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. Обратная задача по определению кинетического коэффициента в модели фильтрац ii tom tatu sf ma’ruzalar to‘plami 9 aprel 2022-yil 11-13.
4. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. Идентификация коэффициента кинетики в модели фильтрации суспензии в пористой среде халқаро илмий-амалий анжуман материаллари 2022 йил, 11-12 май 360-361.
5. Eshquvvat o'g'li.M.S, Shodiyor o'g'li.Sh.J, Raxmonqul o'g'li.A.T, Ma'lumotlarni sinflashtirishda birch algoritmi ahamiyati Часть-11 Том-1 Декабрь -2023 39-42.
6. ME Sanayev, AA Quchqorov Classification of computer application software, European journal of business startups and open society Дата 2024/3/10, том 4, номер 3, страницы 62-65.
7. ME Sanayev, OF Orifov method oriented practical software classification Miasto Przyszłości 46, 210-213.
8. ME Sanayev, OF Orifov The role of text editors in editing and processing text information, European journal of innovation in nonformal education 4(3),43-47
9. SM Eshquvvat o’g’li, Kompyuter amaliy dasturiy ta’minoti tasnifi, Journal of new century innovations 48 (1), 3-8.
10. ME Санаев, КТ Бегмаматов, Топология и современные типы компьютерных сетей, Журнал, Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.

11. ME Sanayev, The role, purpose and functions of information and communication technologies and systems in the economy in the process of modern education, Журнал, Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
12. ME Sanayev, Comparative analysis of the windows operating system, Журнал, Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17, Номер 1.
13. ME Sanayev, AI Ismoilov, Analysis of modern operating systems, Журнал Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
14. ME Sanayev, MB Shaymanov, Modern information technology infrastructure parts, Журнал Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
15. ME Sanayev, AI Ismoilov, The development tendencies of software products in the management of business processes in the economy, Журнал Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17, Номер 1.
16. ME Sanayev, FS Tovbayev, Familiarity with the basic concepts and features of the windows operating system, Журнал Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17 Номер 1.
17. ME Sanayev, Mobil operasion tizimlar tahlili, Журнал "germany" modern scientific research: achievements, innovations and development prospects, Дата 2024/4/20 Том 17 Номер 1.
18. ME Sanayev, AA Quchqorov, The Role of Social Networks in Human Life, Miasto Przyszłości 46, 340-341.
19. SM Eshquvvat o'g'li, Kompyuter dasturiy ta'minotiga bo'lgan talablarini tizimli tahlil qilish, Miasto Przyszłości 46, 262-265.
20. ME Sanayev, Kiber xafsizlik tushunchasi va uning vazifalari, Экономика и социум, 613-619.
21. ME Sanayev, Identifikasiya va autentifikatsiya, Экономика и социум, 620-626.