Содержание:

ВВЕДЕНИЕ

Начиная с 1951 года, когда Джоном фон Нейманом был предложен метод создания самовоспроизводящихся систем, мировая общественность получила в руки новое развлечение. На основе данного метода писали необычные игры («Darwin», «ANIMAL»), программы-шутки и программы-розыгрыши. Однако, начиная с 1981 года шутки выходят из-под контроля, превращаясь в то, что в 1984 в статье Фреда Коэна примет ныне общепринятое название - «компьютерный вирус».

По данным «Лаборатории Касперского», только за первый квартал 2019 года было отражено 843 096 461 атак, проводившихся только с интернет-ресурсов, а это еще далеко не всё, что на сегодняшний день угрожает пользователям различной электронной техники. Таким образом, каждому пользователю необходимо знать, с чем он может столкнуться, с какими видами угроз, дабы, исходя из полученной информации, верно выстроить свою защиту. В этом заключается актуальность темы, раскрываемой в реферате.

Целью реферата является изучение классификации компьютерных вирусов и ознакомление с некоторыми их характеристиками.

Поставленная цель достигается решением следующих задач:

-определением компьютерного вируса;

-ознакомлением с процессом заражения;

-ознакомлением с некоторыми видами вирусов;

Определение компьютерного вируса

Прежде чем приступать к классификации, стоит выяснить, что такое компьютерный вирус в современном понимании.

Компьютерным вирусом называется программа, которая обладает способностью создавать свои копии, и внедрять их в различные объекты и ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения. Пишется подобная программа с целью шутки, вреда чьему-либо компьютеру, получения доступа к компьютеру, перехвата паролей или вымогания денег.

Физическая структура компьютерного вируса достаточно проста. Он состоит из головы и, возможно, хвоста. Под головой вируса понимается компонента, получающая управление первой. Хвост – это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называют несегментированными, тогда как вирусы, содержащие голову и хвост, — сегментированными.

Процесс заражения

Заражение программы, как правило, выполняется таким образом, чтобы вирус получил управление раньше самой программы. Он либо встраивается в начало программы, либо имплантируется в неё так, что первой командой зараженной программы является безусловный переход на компьютерный вирус, текст которого заканчивается аналогичной командой безусловного перехода на команду вирусоносителя, бывшую первой до заражения. Далее вирус выбирает следующий файл, заражает его, возможно, выполняет какие-либо другие действия, после чего снова отдает управление вирусоносителю.

Первичное заражение происходит в процессе наступления инфицированных программ из памяти одной машины в память другой, причем в качестве средства перемещения этих программ могут использоваться как носители информации (оптические диски, флэш-память и т.п.), так и каналы вычислительных сетей. Вирусы, использующие для размножения сетевые средства, сетевые протоколы, управляющие команды компьютерных сетей и электронной почты, принято называть сетевыми.

Цикл жизни вируса обычно включает следующие периоды: внедрение, инкубационный, репликации (саморазмножения) и проявления. В течение инкубационного периода вирус пассивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например необратимую коррекцию информации в компьютере или на

внешних носителях.

Итак, приступим к классификации компьютерных видов.

Классификация по среде обитания вируса

По среде обитания вирусы подразделяются на:

Файловые вирусы — вирусы поражающие исполняемые файлы, написанные в различных форматах. Соответственно в зависимости от формата, в котором написана программа это будут EXE или COM вирусы.

Загрузочные вирусы — вирусы поражающие загрузочные сектора (Boot сектора) дисков или сектор содержащий системный загрузчик(Master Boot Record) винчестера.

Сетевые вирусы — вирусы, распространяющиеся в различных компьютерных сетях и системах.

Макро вирусы — вирусы поражающие файлы Microsoft Office

Flash вирусы — вирусы поражающие микросхемы FLASH памяти BIOS.

Классификация по способу заражения

По способу заражения вирусы делятся на:

Резидентные вирусы — вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти. Они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы. Эти вирусы могут оставаться активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы — вирусы, не оставляющие своих резидентных частей в оперативной памяти компьютера. Некоторые вирусы оставляют в памяти некоторые свои фрагменты не способные к дальнейшему размножению такие вирусы считаются не резидентными.

Классификация по деструктивным возможностям

По деструктивным возможностям вирусы подразделяются на:

Безвредные вирусы — это вирусы ни как не влияющие на работу компьютера за исключение, быть может, уменьшения свободного места на диске и объема оперативной памяти.

Неопасные вирусы — вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий.

Опасные вирусы — это вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей.

Очень опасные вирусы — это вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом.

Классификация по особенностям алгоритма работы

По особенностям алгоритма работы вирусы можно подразделить на:

Вирусы спутники(companion) — эти вирусы поражают EXE-файлы путем создания COM-файла двойника, и поэтому при запуске программы запустится, сначала COM-файл с вирусом, после выполнения своей работы вирус запустит EXE-файл. При таком способе заражения «инфицированная» программа не изменяется.

Вирусы «черви» (Worms) — вирусы, которые распространяются в компьютерных сетях. Они проникают в память компьютера из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии. Иногда они оставляют временные файлы на компьютере но некоторые могут и не затрагивать ресурсы компьютера за исключением оперативной памяти и разумеется процессора.

«Паразитические» — все вирусы, которые модифицируют содержимое файлов или секторов на диске. К этой категории относятся все вирусы не являются вирусами-спутниками и вирусами червями.

«Стелс-вирусы» (вирусы-невидимки, stealth) — представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков подставляют вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

«Полиморфные» (самошифрующиеся или вирусы-призраки, polymorphic) — вирусы, достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

«Макро-вирусы» — вирусы этого семейства используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро-вирусы, заражающие текстовые документы редактора Microsoft Word.

Классификация по режиму функционирования

По режиму функционирования:

— резидентные вирусы (вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам);

— транзитные вирусы (вирусы, которые выполняются только в момент запуска зараженной программы).

Классификация по объекту внедрения

По объекту внедрения:

— файловые вирусы (вирусы, заражающие файлы с программами);

— загрузочные вирусы (вирусы, заражающие программы, хранящиеся в системных областях дисков).

Классификация по объекту заражения

В свою очередь, файловые вирусы подразделяются на вирусы, заражающие:

— исполняемые файлы;

— командные файлы и файлы конфигурации;

— составляемые на макроязыках программирования, или файлы, содержащие макросы (макровирусы — разновидность компьютерных вирусов разработанных на

макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office);

— файлы с драйверами устройств;

— файлы с библиотеками исходных, объектных, загрузочных и оверлейных модулей, библиотеками динамической компоновки и т.п.

Загрузочные вирусы подразделяются на вирусы, заражающие:

— системный загрузчик, расположенный в загрузочном секторе и логических дисков;

— внесистемный загрузчик, расположенный в загрузочном секторе жестких дисков.

Классификация по способу маскировки

По степени и способу маскировки:

— вирусы, не использующие средств маскировки;

— stealth-вирусы (вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных);

— вирусы-мутанты (MtE-вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса).

Классификация MtE-вирусов

В свою очередь, MtE-вирусы делятся:

— на обычные вирусы-мутанты, в разных копиях которых различаются только зашифрованные тела, а дешифрованные тела вирусов совпадают;

— полиморфные вирусы, в разных копиях которых различаются не только зашифрованные тела, но и их дешифрованные тела.

ВЫВОД

Итак, мы рассмотрели некоторые классификации компьютерных вирусов. Цель реферата достигнута. Руководствуясь полученным знанием, будет на порядок проще выстроить оборону своих устройств. А так же, зная, какие виды опасностей

могут встретиться в интернете, постараться их обойти.

Библиографический список

1. https://hitechnic31.ru/klassifikaciya-kompyuternyh-virusov/

2. https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

3.https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%

4. https://securelist.ru/it-threat-evolution-q1-2019-statistics/94021/