Муниципальное автономное общеобразовательное учреждение
“Школа №10 г. Благовещенска”

Индивидуальный итоговый проект

На тему:

“Эволюция компьютерного вируса”

Выполнил:

Кузьмин Роман Евгеньевич

Ученик 9В класса МАОУ

“Школа №10 г. Благовещенска”

Руководитель проекта учитель информатики:

Юнина Дарья Сергеевна

г.Благовещенск

2022

Содержание

Введение

Актуальность: Сегодня широко пользуются персональные компьютеры. Компьютеры нашли свое применение дома, на различных предприятиях, на производстве, в государственных учреждениях, в медицине и т.д. Именно развитие и распространение персональных компьютеров сподвигло появлению программ-вирусов, которые в свою очередь препятствуют нормальной работе компьютеров, разрушают их файловую структуру дисков и наносят ущерб хранимой на них информации.

Цель проекта: Проследить хронологию появления вирусов, выяснить способы защиты от вирусов, а также составить кроссворд по данной теме, тем самым привить интерес людей к информатике.

Задачи: 1. Изучить информацию и литературу по данной теме.

2. Изучить хронологию появления вирусов.

3. Изучить способы защиты от вирусов.

4. Составить кроссворд по теме.

Глава 1

1.1 Компьютерный вирус и его классификации

Компьютерный вирус - вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

Этимология названия

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом в фантастическом рассказе «Человек в шармах», опубликованном в журнале Venture в мае 1970 года.

Термин «компьютерный вирус» впоследствии не раз «открывался» и переоткрывался. Так, переменная в программе PERVADE (1957), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также вирус назвал свои программы Джо Деллинджер, и, вероятно, это и было то, что впервые было правильно обозначено как вирус.

Классификация компьютерных вирусов

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через локальные и глобальные (Интернет) сети. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

По поражаемым объектам. (Файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

Файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.

По поражаемым операционным системам и платформам. (DOS, Windows, Unix, Linux, Android)

По используемым технологиям. (Полиморфные вирусы, стелс-вирусы, руткиты)

По языку, на котором написан вирус. (Ассемблер, высокоуровневый язык программирования, сценарный язык и др.)

По дополнительной вредоносной функциональности. (Бекдоры, кейлоггеры, шпионы, ботнеты и и др.)

1.2 Распространение компьютерных вирусов

Механизм

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение: вписывая себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск через реестр и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически выполняемые команды, - например пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook). Для чего распространители внедряют его в обычные данные (картинки, тексты и т.д) вместе с эксплойтом, использующим уязвимости.

После того как вирус успешно внедрился в коды программы, файла или документа, он будет находиться в состоянии сна, пока обстоятельства не заставят компьютер или устройство выполнить его код. Чтобы вирус заразил ваш компьютер, необходимо запустить заражённую программу, которая, в свою очередь, приведёт к выполнению кода вируса. Это означает, что вирус может оставаться бездействующим на компьютере без каких-либо симптомов поражения. Однако, как только вирус начинает действовать, он может заражать другие файлы и компьютеры, находящиеся в одной сети. В зависимости от целей программиста-вирусописателя, вирусы либо причиняют незначительный вред, либо имеют разрушительный эффект, например удаление данных или кража конфиденциальной информации.

Каналы

1.Дискеты. Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

2.Флеш-накопители («флешки»). В настоящее время USB-накопители заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые камеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны. Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно

указать программу, запускаемую Проводником Windows при открытии такого накопителя. В Windows 7 возможность автозапуска файлов с переносных носителей была отключена.

3.Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

4.Системы обмены мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы обмена мгновенными сообщениями.

5.Веб-сайты. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используется уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

6.Интернет и локальные сети (черви). Черви – вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости – это ошибки и недоработки в программном обеспечении, которые позволяют удалённо загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действие по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

1.3 Вирусная хронология

1. Первый вирус

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ. Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившийся в 1981 году.

Зимой 1984 года появились первые антивирусные утилиты – CHK4BOMB и BOMBSQAD авторства Энди Хопкинса. В начале 1985 года Ги Вон написал программу DPROTECT – первый резидентный вирус.

2.Вирусы 80-х годов 20 века

Первые вирусные эпидемии относятся к 1986 – 1989 годам: Brain (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию), Jerusalem (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).

Тогда же оформляются основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990)

Параллельно оформляются организованные движения как про-, так и антивирусной направленности: в 1990 году появляются специализированная BBS Virus Exchange, «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус Symantec Norton AntiVirus.

3.Вирусы 90-х годов 20 века

В несколько последующих лет были окончательно отточены стелс- и полиморфные технологии (SMEG.Pathogen, SMEG.Queeg, OneHalf, 1994; NightFall, Nostradamus, Nutcracker, 1995), а также испробованы самые необычные способы проникновения в систему и заражения файлов (Dir II — 1991, PMBS, Shadowgard, Cruncher — 1993). Кроме того, появились вирусы, заражающие объектные файлы (Shifter, 1994) и исходные тексты программ (SrcVir, 1994). С распространением пакета Microsoft Office получили распространение макровирусы (Concept, 1995)

В 1996 году появился первый вирус для Windows 95 — Win95.Boza, а в декабре того же года — первый резидентный вирус для неё — Win95.Punch.

С распространением сетей и Интернета файловые ресурсы все больше ориентируются на них как на основной канал работы (ShareFun, 1997 — макровирус MS Word, использующий MS-Mail для распространения; Win32.HLLP.DeTroie, 1998 — семейство вирусов-шпионов; Melissa, 1999 — макровирус и сетевой червь, побивший все рекорды по скорости распространения). Эру расцвета «троянских коней» открывает утилита скрытого удалённого администрирования Black Orifice (1998) и последовавшие за ней аналоги, например NetBus.

Вирус Win95.CIH достиг апогея в применении необычных методов, перезаписывая FlashBIOS заражённых машин (эпидемия в июне 1998 считается самой разрушительной за предшествующие годы).

В конце 1990-х — начале 2000-х годов с усложнением ПО и системного окружения, массовым переходом на сравнительно защищённые Windows семейства NT, закреплением сетей как основного канала обмена данными, а также успехами антивирусных технологий в обнаружении вирусов, построенных по сложным алгоритмам, последние стали всё больше заменять внедрение в файлы на внедрение в операционную систему (необычный, автозапуск, руткиты) и подменять полиморфизм огромным количеством видов (число известных вирусов растет экспоненциально.

4. Вирусы нашего времени

Вместе с тем обнаружение в Windows и другом распространённом ПО многочисленных уязвимостей открыло дорогу червям-эксплойтам. В 2004 году беспрецедентные по масштабам эпидемии вызывают Blaster (по данным Microsoft, более 16 млн систем), Sasser и Mydoom (оценочные ущербы 500 млн и 38 млрд долл. соответственно)

Кроме того, монолитные вирусы в значительной мере уступают место комплексам вредоносного ПО с разделением ролей и вспомогательными средствами (троянские программы, загрузчики/дропперы, фишинговые сайты, спам-боты и пауки). Также расцветают социальные технологии – спам и фишинг – как средство заражения в обход механизмов защиты ПО.

В начале на основе троянских программ, а с развитием технологий p2p-сетей – и самостоятельно – набирает обороты самый современный вид вирусов – черви-ботнеты (Rustock, 2006, ок. 150 тыс. ботов; Conficker, 2008-2009, более 7 млн ботов; Kraken, 2009, ок. 500 тыс. ботов). Вирусы в числе прочего вредоносного ПО окончательно оформляются как средство киберпреступности.

1.4 Признаки появления вируса на ПК

При заражении компьютера могут появиться следующие признаки:

1. На компьютере могут появляться неожиданные сообщения, изображения или звуковые сигналы.
2. Программы без вашего участия могут запускаться или подключаться к интернету.
3. Друзьям на почту или через мессенджер приходят сообщения, которые вы не отправляли.
4. В вашем почтовом ящике много сообщений без адреса отправителя и темы письма.
5. Компьютер работает медленно или часто зависает.
6. При включении компьютера операционная система не загружается.
7. Файлы и папки могут исчезнуть, или их содержимое может измениться.
8. Всплывает множество системных сообщений об ошибке.
9. Браузер зависает или ведет себя неожиданным образом. Например, вы не можете закрыть вкладку.

1.5 Рекомендация профилактических мер

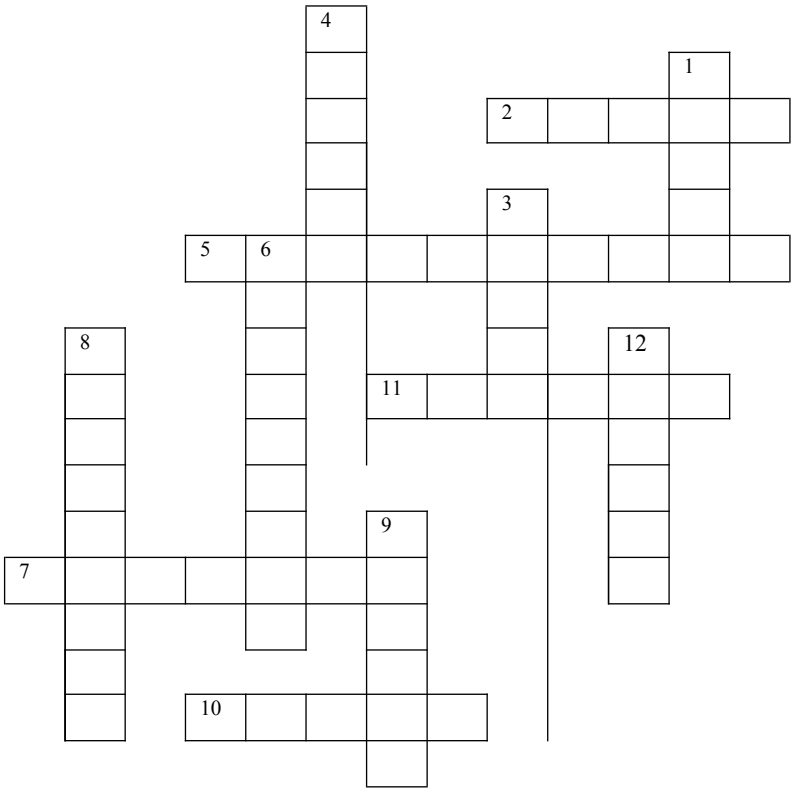
В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учётными записями без крайней необходимости (учётная запись администратора в Windows).
2. Не запускать незнакомые программы из сомнительных источников.
3. Стараться блокировать возможность несанкционированного изменения системных файлов.
4. Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
5. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
6. Пользоваться только доверенными дистрибутивами.
7. Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
8. Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Глава 2

2.1 Создание кроссворда по теме «Эволюция компьютерного вируса»

В качестве продукта своего проекта, я хочу представить составленный мной кроссворд по теме «Эволюция компьютерного вируса».



По горизонтали:

2. Специалист по взлому защиты программ, с целью незаконного доступа к хранящейся в ней информации.

5. Российский программист, специалист по антивирусной защите, один из основателей собственной лаборатории.

7. Носитель информации, помещенный в квадратный пластмассовый корпус, внутри которого гибкий магнитный диск.

10. Программа, обладающая способностью к размножению, выполняющая нежелательные действия на ПК.

11. Ядро, на базе которого создано семейство Unix-подобных операционных систем.

По вертикали:

1. Разновидность вредоносных программ, самостоятельно распространяющихся через локальные и глобальные компьютерные сети.

3. Вирус, вызвавший первую глобальную вирусную эпидемию в 1986 году.

4. Первый вирусный червь.

6. Язык программирования, понятие которого отображают архитектуру электронно-вычислительной машины.

8. Любая программа для обнаружения вируса.

9. Вирус, ущерб которого составляет 38 млрд. долл. (самый дорогой вирус в плане ущерба)

12. Носитель информации, который подключается к ПК через USB.

2.2 Практическая значимость продукта

Практическая значимость продукта заключается в возможности его использования на уроках информатики на этапе закрепления или контроля учебного материала при изучении темы «Компьютерные вирусы» в 8 классе или в рамках внеурочной деятельности (например, на занятиях факультатива, при проведении предметной недели).

Заключение

В данной работе было посвящено изучение эволюции компьютерных вирусов. Актуальность данной работы подтверждают статистические данные, которые характеризуют уровень распространения компьютерных вирусов, а также жизненные примеры.

Вирусы за свой хронологический путь научились обходить системы безопасности (находя уязвимости), незаметно внедряться в систему, распространяться с молниеносной скоростью по сети и наносить большой вред операционной системе, а также хранимой на ней информации. В этом и заключается их эволюция.

Поэтому разработчикам антивирусного программного обеспечения нужно приспосабливаться к появлению новых технологий у вирусов, усовершенствуя свои антивирусные программы.

Во многом проблемы с заражением компьютеров вирусами связанны с неосведомленностью пользователей, поэтому, по моему мнению, людям стоит просвещаться в данной тематике компьютерных вирусов.

В качестве практической работы я составил свой собственный кроссворд по данной теме. При его решении можно использовать материал, представленный в данной работе.

Список использованных источников

1. **https://ru.wikipedia.org/wiki/Компьютерный_вирус**

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

3.Безруков Н.Н. "Компьютерные вирусы", Москва, Наука, 1991

https://ru.wikipedia.org/wiki/История_компьютерных_вирусов