Столыпинский вестник

Научная статья
Original article
УДК 004.05

КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСЫ

COMPUTER VIRUSES AND ANTIVIRUSES

Козлов Захар Сергеевич, студент, 4 курс факультет «Информационная безопасность телекоммуникационных систем», Поволжский государственный университет телекоммуникаций и информатики, Россия, г. Самара

Kozlov Zakhar Sergeyevich, 4th year student, Faculty of Information Security of Telecommunication Systems, Volga State University of Telecommunications and Informatics, Russia, Samara

Аннотация: Существует множество видов вирусов: вирусы загрузочного сектора, файловые вирусы, черви, троянские кони, макровирусы и т. д. Каждый из них имеет большое количество различных вариантов. Сегодня вирусы передаются в большинстве случаев через компьютерные сети и электронную почту. Макровирусы наиболее распространены в настоящее время. Вирусы пытаются использовать неоднозначности операционной системы, прикладных программ, сокетов Windows и даже антивирусных программ. Некоторые вирусы настолько опасны, что делают систему полностью непригодной для использования. В настоящее время обнаружение компьютерных вирусов стало обычным делом. В научной работе описывается

принцип, по которому работают вирусы, как они распространяются с одного компьютера на другой и методы борьбы с ними.

S u m m a r y: There are many types of viruses: boot sector viruses, file viruses, worms, Trojan, macro viruses, etc. Each of them has many different options. Today, viruses are transmitted in most cases through computer networks and e-mail. Macro viruses are the most common now. Viruses try to exploit ambiguities of the operating system, application programs, Windows sockets, and even antivirus programs. Some viruses are so dangerous that they make the system completely unusable. Nowadays, the detection of computer viruses has become commonplace. The scientific work describes the principle by which viruses work, how they spread from one computer to another and methods of combating them.

Ключевые слова: вирус, антивирусные программы, электронная почта, Windows, компьютерные сети, червь, троян, макровирус.

Keywords: virus, antivirus programs, e-mail, windows, computer networks, worm, trojan, macro viruses

Введение

Компьютерные вирусы являются вредоносными программами, которые способны заразить компьютер и замедлить его работу или завладеть конфиденциальной информацией пользователя, а также они способны распространяться на другие узлы в локальной или глобальной компьютерной сети. Компьютерные вирусы обычно имеют небольшие размеры, которые предназначены для распространения с одного компьютера на другой, проникновения и вмешательства в работу машины [4;6]. Червь или троян немного отличаются от других типов вирусов, они прикрываются под видом рабочей программы без вирусов. Вирус может повредить или удалить важные данные на вашем компьютере. Вирус распространяется через электронную почту, флэш-накопители, веб-сайты, нелицензированное программное обеспечение. В данной статье рассматривается, во-первых, основной принцип работы вируса и различные известные вирусы, во-вторых, как вирус

распространяется и, наконец, шаги, которые могут помочь решить эту проблему [1;3].

Цель исследования

Необходимо проанализировать основные типы компьютерных вирусов, принцип их работы и методы распространения. Так же рассмотреть методы защиты от компьютерных вирусов, одним из которых является антивирус.

Методы исследования

Работа проводилась с использованием методов исследования: сравнения и анализа.

Основная часть

1. Принцип действия распространенных компьютерных вирусов

Компьютерный вирус известен как вредоносный код, предназначенный для нанесения ущерба компьютерам.

Наиболее распространенные вредоносные коды:

Вирусы — это часть программного обеспечения, которая использует обычные программы. Например, он может подключаться к программе для работы с электронными таблицами. Всякий раз, когда запускается данная программа, запускается и вирус, который имеет способность размножаться, подключившись к другим программам и наносить ущерб.

Троянский конь: компьютерная программа с вредоносным кодом, которая маскирует свою истинную функцию наносить вред компьютеру пользователя, при ее запуске. Данные вирусы могут использоваться для установления контроля над зараженным компьютером, удаления данных пользователя, запуск других вредоносных программ и установления бэкдоров (программное обеспечение, служащее для дистанционного доступа к зараженному устройству).

Одним из распространенных вирусов троянов это Cryptolocker. Распространяется с помощью зараженных вложений электронной почты. Электронное сообщение содержит зараженный ZIP-файл, с паролем. Пользователь открывает ZIP-архив, используя пароль, и открывает в архиве

PDF-файл, троян активируется. Он ищет файлы для шифрования на локальных дисках и подключенных сетевых дисках и шифрует файлы, используя асимметричное шифрование с 1024- или 2048-битными ключами [5].

Сетевые черви: червь представляет собой небольшую программу, которая использует компьютерные сети и средства безопасности для собственного воспроизведения. Копия червя сканирует сеть в поисках другой машины, имеющей определенную брешь в системе безопасности. Далее червь копирует себя на новую машину, используя брешь, а затем также начинает реплицироваться оттуда. На зараженных компьютерах он может оставлять бэкдор. Таким образом, программный червь — это вредоносная программа, самостоятельно распространяющаяся через локальные или глобальный компьютерные сети.

Одним из самых популярных вирусов-червей является ILOVEYOU. Он распространялся как фишинговое письмо с вложением «ILOVEYOU», которое оказалось текстовым файлом. Получатели открывали вложение, заражались, вирус перезаписывал файлы на машине, а затем рассылал себя всему их списку контактов. Этот простой, но эффективный метод распространения привел к тому, что вирус распространился на миллионы компьютеров.

1.1 Другие типы вирусов

Файловый вирус: он заражает систему, добавляя себя в начало, конец или середину исполняемого файла формата EXE, COM, динамические библиотеки DLL и т. п. Получив управление, вирус может выполнять деструктивные действия, заданные алгоритмом вируса, заражать другие файлы компьютера или его оперативную память. Его также называют паразитическим вирусом, потому что он не оставляет нетронутым ни один файл.

Вирус загрузочного сектора: он заражает загрузочный сектор жесткого диска, запускаясь всякий раз, когда система загружается, но перед полной загрузкой самой ОС. Размножается вирус записью в загрузочную область

прочих накопителей в компьютере. Он также называются вирусом памяти, поскольку он не заражают файловую систему.

Макровирус: большинство вирусов написано на языке низкого уровня, таком как C или язык ассемблера. Этот вирус был написан на ориентированном на приложения языке, таком как Visual Basic. Эти вирусы запускаются при запуске программы, способной выполнять макрос. Например, макровирус часто содержится в файлах электронных таблиц. Макрос — это программный алгоритм действий, составленный пользователем.

Полиморфный вирус: это шаблон, который идентифицирует вирус или серию байтов, которые структурируют вирусный код, чтобы избежать обнаружения антивирусом. Постоянное видоизменение программного вредоносного кода позволяет вирусу оставаться почти незамеченным. Функциональность вируса остается прежней, но его сигнатура изменяется.

Вирус-шифровальщик: вредоносный код, который ищет на диске ценную информацию, например документы, таблицы, изображения и шифрует все, что сумел найти. Зашифрованные файлы невозможно открыть и использовать. После этого вирус-шифровальщик выводит на экран сообщение с требованием выкупа за восстановление вашей информации. Источником данного вируса могут послужить электронные письма с прикрепленными файлами, со ссылками на вредоносные сайты.

Туннельный вирус: этот вирус избегает обнаружения антивирусным сканером, устанавливаясь в цепочке обработчиков прерываний. Программы перехвата остаются в фоновом режиме операционной системы и перехватывают вирусы, которые отключаются во время туннелирования вируса. Подобные вирусы устанавливаются в драйверах устройств.

Многосторонний вирус: он может заразить несколько частей системы, включая загрузочный сектор, память и файлы. Его трудно обнаружить и сдержать.

2. Как происходит вирусная атака?

Вирус, прикрепленный к программе, файлу или документу может быть неактивен. Он будет скрыт до тех пор, пока обстоятельства не заставят компьютер или устройство выполнить его код. Вирус может оставаться бездействующим на вашем компьютере, не проявляя серьезных признаков или симптомов. Однако, как только вирус заражает ваш компьютер, он может заразить и другие компьютеры в аналогичной сети. Возможные последствия от вируса — это кража паролей или данных, регистрация нажатий клавиш, повреждение файлов, шпионаж через веб-камеру, рассылка спама по электронной почте и контактам. Вирусы часто распространяются через вложения электронной почты и текстовых сообщений, загрузки файлов из Интернета и мошеннические ссылки в социальных сетях. Мобильные устройства и смартфоны заражаются вирусами при загрузке приложений. Вирусы могут скрываться под видом вложений с общедоступным контентом, таким как забавные картинки, поздравительные открытки или аудио- и видеофайлы. В то время как некоторые вирусы часто имеют игривые намерения и последствия, другие могут оказывать глубокое и разрушительное воздействие. Это включает в себя стирание данных или повреждение вашего жесткого диска. В худших случаях некоторые вирусы разрабатываются с финансовой выгодой.

2.1 Признаки компьютерного вируса

Вирус может вызывать несколько симптомов. Некоторые из них заключаются в следующем. Частые всплывающие окна, некоторые всплывающие сообщения побуждают вас перейти на необычные сайты. В качестве альтернативы они могут попросить вас загрузить антивирус или другие программы.

Массовые электронные письма, отправленные с вашей учетной записи электронной почты. Преступник может завладеть вашей учетной записью или отправлять электронные письма от вашего имени с другого зараженного компьютера.

Частые сбои могут быть признаком вируса, который может нанести серьезный ущерб вашему дисководу. Это может привести к зависанию вашего устройства.

Необычно низкая производительность компьютера. Внезапное изменение скорости обработки может сигнализировать о том, что ваш компьютер заражен вирусом.

Неизвестные программы, которые запускаются после активации компьютера. Вы узнаете о незнакомой программе, как только запускаете свой компьютер. В противном случае вы можете заметить это, проверив список активных приложений вашего компьютера [8].

Необычные действия, такие как смена пароля. Это может помешать вам войти в учетную запись своего компьютера.

3. Источники компьютерных вирусов

Вирусные атаки участились по всему миру. Мы должны позаботиться обо всех возможных способах защиты от вредоносных атак.

Несколько наиболее распространенных источников вирусных атак.

3.1. Загрузка программ

Программы, содержащие загружаемые файлы, являются наиболее типичным источником вредоносных программ, такие как бесплатные программы и другие исполняемые файлы. Независимо от того, загружаете ли вы программу для редактирования изображений, музыкальный файл или электронную книгу. Всякий раз, старайтесь избегать загрузок файлов с неизвестных или непопулярных источников в интернете.

3.2. Взломанное программное обеспечение

Всякий раз, когда вы открываете взломанное программное обеспечение, ваше антивирусное программное обеспечение может пометить его как вредоносное ПО, поскольку взломы содержат вредоносные скрипты. Всегда говорите: “Нет” взломам, так как они будут внедрять вредоносный скрипт в ваш компьютер.

3.3. Вложения электронной почты

Любой желающий может отправить вам вложение по электронной почте, независимо от того, узнаете вы его или ее или нет. Нажатие на неизвестные ссылки или вложения может привести к повреждению вашей системы. Подумайте, прежде чем нажимать на что-либо, и убедитесь, что тип файла не “.exe”.

3.4. Веб-сайт

Один из самых простых способов взаимодействия с вашим устройством - через Интернет. Подтвердите URL-адрес (Единый локатор ресурсов) перед доступом к любому веб-сайту. Для определения защищенного URL-адреса всегда ищите в нем “https”. Как только вы нажмете на видео, опубликованное в социальных сетях, веб-сайт может потребовать, чтобы вы установили определенный тип плагина для просмотра этого видео. Этот плагин может быть вредоносным программным обеспечением, которое украдет вашу конфиденциальную информацию.

3.5. Bluetooth

Передача данных по Bluetooth может заразить вашу систему, поэтому крайне важно понимать, какой тип медиафайла отправляется на ваш компьютер всякий раз, когда происходит передача. Эффективным решением было бы разрешить подключение по Bluetooth только к известным устройствам и активировать его только при необходимости.

Помимо вышеупомянутых источников, файлообменные сети также являются источником атак.

4. Защита от вирусов

Существует несколько способов, с помощью которых мы можем защитить нашу систему и данные от вирусного воздействия.

4.1. Поддерживайте свое программное обеспечение в актуальном состоянии

Компании-разработчики программного обеспечения, такие как Microsoft и Oracle, регулярно обновляют свое программное обеспечение для устранения

ошибок. Неактуальность версии программного обеспечения может быть использовано вирусом для возможности заражения компьютера.

4.2. Не переходите по ссылкам в электронных письмах

Хорошее эмпирическое правило заключается в том, что если вы не узнаете отправителя электронного письма, то не нажимайте ни на какие ссылки в письме.

4.3. Используйте бесплатное или платное антивирусное программное обеспечение

Вам не нужно покупать программное обеспечение для защиты вашего компьютера или годовую подписку, чтобы позаботиться о новейшей защите от вирусов. Для пользователей Windows Microsoft Security Essentials бесплатна. Avast — это еще одна бесплатная антивирусная программа.

4.4. Резервная копия данных

Если у вас нет защиты системы, то вы должны периодически делать резервную копию своих данных. Три основных варианта резервного копирования: Внешний накопитель, Онлайн-служба резервного копирования, Облачное хранилище. Используйте такие услуги, как Google drive, Google docs для хранения файлов. Некоторые облачные хранилища имеют определенный бесплатный объем хранения данных. Виртуальное хранилище — это ресурс для сохранения ваших данных

4.5. Пароль

В то время как некоторые люди используют эквивалентный пароль для всего, избегайте этой практики. Длина пароля должна составлять не менее восьми символов. Надежный пароль, состоит из букв, цифр и символов. Периодически меняйте свой пароль.

4.6. Брандмауэр

Если в вашей системе запущено антивирусное программное обеспечение, то это не значит, что у вас есть брандмауэр. Компьютеры на базе ОС Windows и IOS имеют встроенное программное обеспечение брандмауэра. Убедитесь, что он включен.

4.7. Блокировщик всплывающих окон

Веб-браузеры имеют возможность предотвращать всплывание окон. Вы можете использовать Add Blocker, чтобы заблокировать вредоносную и навязчивую рекламу на веб-сайтах.

5. Антивирус

5.1. Что такое антивирусное программное обеспечение?

Антивирусное программное обеспечение обнаруживает и удаляет вирусы и другие вредоносные программы, такие как черви, трояны, рекламное ПО и многое другое. Это программное обеспечение предназначено для использования в качестве превентивного подхода к кибербезопасности, чтобы остановить угрозы до того, как они попадут на ваш компьютер и вызовут проблемы.

5.2. Принцип работы антивируса

Антивирусное программное обеспечение работает, сканируя входящие файлы или код, который передается через сетевой трафик. Компании, которые создают это программное обеспечение, составляют обширную базу данных уже известных вирусов и вредоносных программ и регулярно обновляют ее. Когда файлы, программы и приложения передаются на ваш компьютер, антивирус сравнивает их со своей базой данных, чтобы найти совпадения. Совпадения, похожие или идентичные базе данных, изолируются в карантин, сканируются и удаляются. В режиме реального времени, когда вы просматриваете веб-страницы, отправляете электронные письма, смотрите потоковое видео или делаете что-либо еще в Интернете, программное обеспечение предупредит вас, чтобы вы не нажимали на какие-либо веб-сайты или файлы, которые могут представлять угрозу вашей безопасности в Интернете.

5.3. Отличия бесплатных и платных антивирусов

Функции платных антивирусов дают вам возможности большего контроля своих личных данных и повышают надежность защиты информации. Защита от спама, родительский контроль, хранение паролей, более

эффективное обеспечение безопасности онлайн-платежей, резервное копирование, очистка компьютера и дополнительные уровни безопасности данных пользователя так же входят в пакет услуг платных антивирусов. Бесплатные антивирусы обеспечивают базовую защиту от вирусов, а платные предлагают более надежную защиту [7].

5.4. Популярное антивирусное программное обеспечение

По данным исследовательского портала US News 360 Reviews на 13 июня 2022 год составлен рейтинг популярных антивирусных программ для Windows 11 и Windows 10:

1. Bitdefender. Цена от 40 долларов и выше. Присутствует бесплатная версия.
2. Norton. Цена от 60 долларов и выше. Бесплатная версия отсутствует.
3. Kaspersky. Цена от 60 долларов и выше. Присутствует бесплатная версия.
4. ESET. Цена от 40 долларов и выше. Бесплатная версия отсутствует.
5. Webroot. Цена от 40 долларов и выше. Присутствует бесплатная версия.

Результаты

Были рассмотрены основные типы компьютерных вирусов, их действия и методы распространения. Также рассмотрены способы защиты от них и разобран принцип работы компьютерных антивирусов.

Заключение

Были выявлены угрозы в лице компьютерных вирусов, которые несли опасность нарушения работы компьютеров и риск кражи конфиденциальной информации пользователей.

Цель достигнута и были рассмотрены методы противодействия вирусным угрозам. Например, антивирусное программное обеспечение. Необходимо, чтобы конфиденциальная информация пользователя,

хранящаяся на его персональном компьютере, была доступна только ему и лицам, которым он доверяет.

Литература

1. Афанасьева Д. В. Сравнительный анализ антивирусного программного обеспечения //Известия Тульского государственного университета. Технические науки. 2021. №. 5. С. 216–218.
2. Кобзистов А. В., Кондратьев В. Ю. Антивирусное программное обеспечение //Информационное общество: современное состояние и перспективы развития. 2016. С. 103–106.
3. Курманбай А. К. Обзор и сравнение антивирусного программного обеспечения //Ресурсоэффективным технологиям-энергию и энтузиазм молодых: сборник научных трудов VI Всероссийской конференции, г. Томск, 22–24 апреля 2015 г.Томск, 2015. С. 64–68.
4. Афанасьева Д. В. Компьютерные вирусы: специфика и противодействие //Наука, образование и культура. 2019. №. 3 (37). С. 11–12.
5. Атамкулова М. Т., Саримсаков А. А. Компьютерные вирусы и антивирусные программы //Известия Ошского технологического университета. 2016. Т. 2. С. 136–140.
6. Горчицин А. А. Компьютерные вирусы //Аллея науки. – 2017. – Т. 2. №. 10. С. 72–75.
7. Блазуцкая Е. Ю., Шарафутдинов А. Г. Вирусы нового поколения и антивирусы //NovaInfo. Ru. 2015. Т. 1. №. 35. С. 92–94.
8. Ганижева Н. Ж. Компьютерные вирусы и антивирусные программы //Молодой ученый. 2021. №. 33. С. 3–5.

Literature

1. Afanasyeva D. V. Comparative analysis of antivirus software //Proceedings of Tula State University. Technical sciences. 2021. No. 5. P. 216–218.
2. Kobzistov A.V., Kondratiev V. Y. Antivirus software //Information society: current state and prospects of development. 2016. P. 103–106.
3. Kurmanbai A. K. Review and comparison of antivirus software //Resource-

efficient technologies-energy and enthusiasm of the young: collection of scientific papers of the VI All-Russian Conference, Tomsk, April 22-24, 2015, Tomsk, 2015. 2015. P. 64–68.

4. Afanasyeva D. V. Computer viruses: specifics and counteraction //Science, education, and culture. 2019. No. 3 (37). P. 11-12.
5. Atamkulova M. T., Sarimsakov A. A. Computer viruses and antivirus programs //Izvestiya Osh Technological University. 2016. Vol. 2. P. 136-140.
6. Gorchitsyn A. A. Computer viruses //Alley of Science. – 2017. – Vol. 2. No. 10. P. 72-75.
7. Blazutskaya E. Yu., Sharafutdinov A. G. New generation viruses and antiviruses //NovaInfo. Ru. 2015. Vol. 1. No. 35. P. 92-94.
8. Ganizheva N. J. Computer viruses and antivirus programs //A young scientist. 2021. No. 33. P. 3-5.

Для цитирования: Козлов З.С. КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСЫ// Научный сетевой журнал «Столыпинский вестник» №4/2022