ЛЕКЦИЯ
«КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ»

ВОПРОСЫ ЛЕКЦИИ:

1. Компьютерные вирусы и защита от них.
2. Классификация компьютерных вирусов.
3. Антивирусные программы.

ЛИТЕРАТУРА:

1. С.Н. Никифоров. Методы защиты информации. Защита от внешних вторжений. Учебное пособие. – СПб.: Лань, 2018. – 96 с.
2. Гошко С.В. Технологии борьбы с компьютерными вирусами [Электронный ресурс]: практическое пособие/ Гошко С.В.— Электрон. текстовые данные.— Москва: СОЛОН-ПРЕСС, 2016. — 351 с. — Режим доступа: http://www.iprbookshop.ru/90288.html. — ЭБС «IPRbooks».
3. Вирусная энциклопедия «Лаборатории Касперского» [электронный ресурс]. URL: https://encyclopedia.kaspersky.ru (Дата обращения: 29.11.2020).

1.Компьютерные вирусы и защита от них.

Компьютерные вирусы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Современный компьютерный вирус – это практически незаметный для обычного пользователя "враг", который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Вирусные эпидемии способны блокировать работу организаций и предприятий.

На тему борьбы с вирусами написаны десятки книг и сотни статей, борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в сотнях компаний. Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

В последнее время вирусные эпидемии стали настолько масштабными и угрожающими, что сообщения о них выходят на первое место в мировых новостях. При этом следует иметь в виду, что антивирусные программы и аппаратные средства не дают полной гарантии защиты от вирусов, а большинство пользователей не имеют даже основных навыков "защиты" от вирусов.

Е. Касперский в своей книге "Компьютерные вирусы" отмечает, что "Борьба с компьютерными вирусами является борьбой человека с человеческим же разумом. Эта борьба является борьбой умов, поскольку задачи, стоящие перед вирусологами, ставят такие же люди :".

Характерные черты компьютерных вирусов

Термин "компьютерный вирус" появился в середине 80-х годов, на одной из конференций по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако, строгого определения компьютерного вируса так и нет.

Трудность, возникающая при попытках сформулировать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения не имеют к вирусам, либо существуют вирусы, которые не содержат

указанных выше отличительных черт (за исключением возможности распространения).

Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса. К более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТе Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения".

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Невозможность четкой формулировки определения компьютерного вируса сама по себе не является проблемой. Главная проблема, которая следует из этого, заключается в том, что нет четких (однозначных) признаков, по которым можно отличить различные файлы от "вирусов", что не позволяет в полной мере устранить их влияние.

Несмотря на все усилия разработчиков антивирусного программного обеспечения до сегодняшнего дня нет достаточно надежных антивирусных средств и, скорее всего, противостояние "вирусописателей" и их оппонентов будет постоянным.

Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может

быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной "компьютерной гигиены".

Хронология развития компьютерных вирусов

Появление первых компьютерных вирусов, способных дописывать себя к файлам, связывают с инцидентом, который произошел в первой половине 70-х годов на системе Univax 1108. Вирус, получивший название "Pervading Animal", дописывал себя к выполняемым файлам – делал практически то же самое, что тысячи современных компьютерных вирусов.

Можно отметить, что в те времена значимые события, связанные с компьютерными вирусами, происходили один раз в несколько лет. С началом 80-х компьютеры становятся все более и более популярными. Появляется все больше и больше программ, начинают развиваться глобальные сети. Результатом этого является появление большого числа разнообразных "троянских коней" – программ, которые при их запуске наносят системе какой-либо вред. В 1986 г. произошла первая эпидемия IBM-PC вируса "Brain". Вирус, заражающий 360Кб дискеты, практически мгновенно разошелся по всему миру. Причиной такого "успеха" являлась, скорее всего, неготовность компьютерного общества к встрече с таким явлением, как компьютерный вирус.

В 1987 г. произошло событие, которое популяризировало "компьютерные вирусы". Код вируса "Vienna" впервые публикуется в книге Ральфа Бюргера "Computer Viruses: A High Tech Desease". Сразу же в 1987 г. появляются несколько вирусов для IBM-PC.

В пятницу 13-го мая 1988-го года сразу несколько фирм и университетов нескольких стран мира "познакомились" с вирусом "Jerusalem" – в этот день вирус уничтожал файлы при их запуске. Вместе с несколькими другими вирусами, вирус "Jerusalem" распространился по тысячам компьютеров, оставаясь незамеченным – антивирусные программы еще не были распространены в то время так же широко как сегодня, а многие пользователи и даже профессионалы еще не верили в существование компьютерных вирусов. Не прошло и полгода, как в ноябре повальная эпидемия сетевого вируса Морриса

(другое название – Internet Worm) заразила более 6000 компьютерных систем в США и практически парализовала их работу. По причине ошибки в коде вируса он неограниченно рассылал свои копии по другим компьютерам сети и, таким образом, полностью забрал под себя ее ресурсы. Общие убытки от вируса Морриса были оценены в 96 миллионов долларов.

В 1992 году появились первые конструкторы вирусов VCL и PS-MPC, которые увеличили и без того немаленький поток новых вирусов. В конце этого года первый вирус для Windows, заражающий выполняемые файлы этой операционной системы, открыл новую страницу компьютерных вирусов.

В дальнейшем развитие компьютерных вирусов напоминает сводку с полей сражений. Создатели вирусов становятся все более изощренными, количество антивирусных программ растет, но ни одна из них не защищает в полной мере. В компьютерном обществе появляется синдром "компьютерного вируса".

К борьбе с вирусами подключаются правоохранительные органы: летом 1994 года автор вируса SMEG был арестован. Примерно в то же самое время в той же Великобритании арестована целая группа вирусописателей, называвшая себя ARCV (Assotiation for Really Cruel Viruses). Некоторое время спустя еще один автор вирусов был арестован в Норвегии.

Август 1995 г. один из поворотных моментов в истории вирусов и антивирусов: обнаружен первый вирус для Microsoft Word ("Concept"). Так начиналось время макровирусов.

В 1998 году появились первые полиморфные Windows32-вирусы-"Win95. HPS" и "Win95. Marburg". Разработчикам антивирусных программ пришлось спешно адаптировать к новым условиям методики детектирования полиморфных вирусов, рассчитанных до того только на DOS-вирусы.

Наиболее заметной в 1998 г. была эпидемия вируса "Win95. CIH", ставшая сначала массовой, затем глобальной, а затем повальной – сообщения о заражении компьютерных сетей и домашних персональных компьютеров исчислялись сотнями, если не тысячами. Начало эпидемии зарегистрировано на

Тайване, где неизвестный заслал зараженные файлы в местные Интернет-конференции.

С середины 90-х годов основным источником вирусов становится глобальная сеть Интернет.

С 1999 года макровирусы начинают постепенно терять свое господство. Это связано со многими факторами. Во-первых, пользователи осознали опасность, таящуюся в простых doc- и xls-файлах. Люди стали более внимательными, научились пользоваться стандартными механизмами защиты от макровирусов, встроенными в MS Office.

В 2000 году происходят очень важные изменения на мировой "вирусной арене". На свет появляется новый тип вредных кодов – сетевые черви. В это же время появляется супервирус – "Чернобыль". "Чернобыль" исполняемый вирус под Windows, имеющий следующие особенности.

Во-первых, зараженный файл не меняет своего размера по сравнению с первоначальным вариантом. Такой эффект достигается благодаря структуре исполняемых файлов Windows: каждый exe-файл разбит на секции, выровненные по строго определенным границам. В результате между секциями почти всегда образуется небольшой зазор. Хотя такая структура приводит к увеличению места, занимаемого файлом на диске, она же позволяет существенно повысить скорость работы операционной системы с таким файлом. "Чернобыль" либо записывает свое тело в один такой зазор, либо дробит свой код на кусочки и копирует каждый из них в пустое место между границами. В результате антивирусу сложнее определить, заражен ли файл или нет, и еще сложнее вылечить инфицированный объект.

Во-вторых, "Чернобыль" стал первопроходцем среди программ, умеющих портить аппаратные средства. Некоторые микросхемы позволяют перезаписывать данные, хранящиеся в их мини ПЗУ. Этим и занимается этот вирус.

2000 год еще можно назвать годом "Любовных Писем". Вирус "LoveLetter", обнаруженный 5 мая, мгновенно разлетелся по всему миру,

поразив десятки миллионов компьютеров практически во всех уголках планеты. Причины этой глобальной эпидемии кроются в чрезвычайно высокой скорости распространения. Вирус рассылал свои копии немедленно после заражения системы по всем адресам электронной почты, найденным в адресной книге почтовой программы Microsoft Outlook. Подобно обнаруженному весной 1999 года вирусу Melissa, LoveLetter это делал, якобы, от имени владельца зараженного компьютера, о чем тот, естественно, даже не догадывался. Немаловажную роль при распространении вируса сыграл и психологический аспект: мало кто сможет удержаться, чтобы не прочитать любовное письмо от своего знакомого. Именно на это была сделана основная ставка в процессе разработки вируса. О масштабах заражения вирусами в начале 21 века свидетельствует тот факт, что только в мае атаке вируса LoveLetter подверглись более 40 миллионов компьютеров. Уже за первые 5 дней эпидемии вирус нанес мировой экономике убытки в размере 6,7 миллиардов долларов.

С 2000 года сетевые черви начинают полностью преобладать на вирусной арене мира. Сегодня, по данным Лаборатории Касперского, на их долю приходится 89,1 % всех заражений. В структуре распространенности сетевых червей традиционно преобладают почтовые, использующие e-mail в качестве основного транспорта для доставки на целевые компьютеры.

В 2001 году был обнаружен новый тип вредоносных кодов, способных активно распространяться и работать на зараженных компьютерах без использования файлов – "бестелесные черви". В процессе работы такие вирусы существуют исключительно в системной памяти, а при передаче на другие компьютеры - в виде специальных пакетов данных.

Такой поворот событий поставил сложные задачи перед разработчиками антивирусных пакетов. Традиционные технологии (антивирусный сканер и монитор) проявили неспособность эффективно противостоять новой угрозе, поскольку их алгоритм борьбы с вредоносными программами основан именно на перехвате файловых операций. Решением проблемы стал специальный антивирусный фильтр, который в фоновом режиме проверяет все поступающие

на компьютер пакеты данных и удаляет "бестелесных" червей. Глобальная эпидемия сетевого червя CodeRed, начавшаяся 20 июля 2001 года, подтвердила действенность технологии "бестелесности". Но еще серьезнее оказалась эпидемия вируса Helkern 25 января 2003 года.

Вирус Sasser создал немало неприятностей в 2004 году, которые вылились в 500 млн долл убытков. К тому же, он уничтожил картографическую систему Британской береговой охраны и спровоцировал отмену ряда авиарейсов. Создателем вируса, причинившего столько вреда, оказался подросток из Германии. Его быстро задержали после того, как один из его «друзей» сдал юного хакера, чтобы получить 250 тыс долл вознаграждения от Microsoft.

Вирус Conficker, в 2007 году заразивший миллионы компьютеров по всему миру, причинил более 9,1 млрд долл убытков. Он проверял компьютеры на наличие слабых мест и уязвимостей, назначал сочетания клавиш и загружал код с хакерских сайтов.

В сентябре 2010 года вирус Stuxnet поразил компьютеры сотрудников АЭС в Бушере (Иран) и создал проблемы в функционировании центрифуг комплекса по обогащению урана в Натанзе. По мнению экспертов, Stuxnet стал первым вирусом, который был использован как кибероружие.

В январе 2013 года эксперты «Лаборатории Касперского» сообщили об обнаружении шпионской сети «Красный октябрь», организаторы которой вели слежку за дипломатическими, правительственными и научными организациями в различных странах. Предполагаемые киберпреступники пытались получить конфиденциальную информацию и данные, дающие доступ к компьютерным системам, персональным мобильным устройствам и корпоративным сетям, а также занимались сбором сведений геополитического характера. Ареал деятельности данных лиц распространялся на республики бывшего СССР, страны Восточной Европы, а также некоторые государства Центральной Азии.

27 июня 2017 года от атаки компьютерного вируса - шифровальщика Petya.A пострадали десятки компаний в РФ и на Украине. По сообщению Group-IB, которая занимается предотвращением и расследованием киберпреступлений,

в России атаке подверглись компьютерные системы "Роснефти", "Башнефти", "Евраза", российских офисов компаний Mars, Mondeles и Nivea. На Украине вирусной атаке подверглись компьютеры "Киевэнерго", "Укрэнерго", "Ощадбанка" и концерна "Антонов". Также из-за вируса временно отключился автоматический мониторинг промышленной площадки на Чернобыльской АЭС. Вирус Petya распространяется через ссылки в сообщениях электронной почты и блокирует доступ пользователя к жесткому диску компьютера, требуя выкуп в размере $300 в биткойнах. Этим он схож с вредоносной программой WannaCry, с которой была связана предыдущая крупная вирусная атака в мае 2017 года.

24 октября 2017 года атаке вируса-вымогателя подверглись компьютеры в РФ, на Украине, в Турции и Германии. По предварительным данным, криптовирус Bad Rabbit (англ. "плохой кролик") послужил причиной недоступности для пользователей сайтов ряда СМИ, в частности - российского агентства "Интерфакс". Кроме того, сообщалось о "хакерской атаке" на информационную систему международного аэропорта Одессы (Украина) и метрополитен Киева.

Вирусы-вымогатели (ransomware, криптовирусы) работают по схожей схеме: они блокируют рабочий стол пользователя компьютера, шифруют все файлы определенных типов, найденные на компьютере, после чего удаляют оригиналы и требуют выкуп (обычно - перевод определенной суммы денежных средств на счет злоумышленников) за ключ, разрешающий продолжить работу и вернуть файлы. Зачастую создатели криптовирусов ставят пользователям жесткие условия по срокам уплаты выкупа, и если владелец файлов не укладывается в эти сроки, ключ удаляется. После этого восстановить файлы становится невозможно.

Как писала газета «Известия», 1 сентября 2020 года, Свердловский областной онкологический диспансер атаковали хакеры. Вирус зашифровал около 400 исследований. В этом учреждении отметили, что они дублируются на бумажных носителях. Ранее сотрудница диспансера Светлана Лаврова на своей странице в Facebook сообщила, что взломщики потребовали 80 тыс. рублей за восстановление информации. В медучреждении заявили, что все данные удалось расшифровать.

Из-за роста в 2020 году популярности IoT-устройств (Internet of Things, интернет вещей), к которым относятся умные колонки и видеозвонки, хакеры ищут новые способы воспользоваться данными устройствами для получения ценной информации. Хакеры выбирают IoT-устройства по нескольким причинам. Во-первых, у большинства IoT-устройств недостаточный объем хранилища для установки надежных средств обеспечения защиты. Данные устройства зачастую содержат данные со слабо защищенным доступом, например пароли и имена пользователей, которыми могут воспользоваться хакеры для входа в аккаунты и кражи ценной информации, например банковских реквизитов.

Хакеры также могут использовать подключенные к интернету камеры и микрофоны для шпионажа и общения с людьми, в том числе с детьми через устройство “видеоняня”. Подобные устройства также могут являться слабым звеном корпоративных сетей – это значит, что хакеры могут получить доступ ко всем системам через IoT-устройства и распространять вредоносные программы по всей сети.

Программы для криптоджекинга (или вредоносного майнинга) используют вычислительные мощности для помощи в “майнинге” криптовалют, например Биткоина. Майнинг задействует значительные вычислительные мощности для создания криптовалюты, поэтому хакеры пытаются установить программы для криптоджекинга на ваши компьютеры и мобильные устройства и ускорить процесс майнинга, при этом значительно замедляя устройства пользователей.

Несмотря на значительный спад криптоджекинга в последние годы, в большей степени из-за падения стоимости криптовалют, данная угроза остается актуальной. Из-за роста цен на криптовалюты в 2020 году, криптоджекинг останется прибыльным видом атак для киберпреступников.

Киберпреступники зачастую тратят на кибератаки много времени и ресурсов. Поэтому с развитием технологий искусственного интеллекта и машинного обучения, в 2020 и последующих годах нам следует ожидать от

хакеров разработки высокотехнологичных и разрушительных вредоносных программ, основанных на искусственном интеллекте.

2. Классификация компьютерных вирусов

По среде "обитания" вирусы делятся на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Файловые вирусы внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы популярных офисных приложений.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии. Другой пример такого сочетания – сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая операционная система является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-

либо одной или нескольких операционных систем. Макровирусы заражают файлы форматов Word, Excel, пакета Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

По особенностям алгоритма работы вирусы делятся на:

- резидентные;
- стелс-вирусы;
- полиморфик-вирусы;
- вирусы, использующие нестандартные приемы.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. К резидентным относятся макровирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие "перезагрузка операционной системы" трактуется как выход из редактора.

В многозадачных операционных системах время "жизни" резидентного вируса также может быть ограничено моментом закрытия зараженного окна, а активность загрузочных вирусов в некоторых операционных системах ограничивается моментом инсталляции дисковых драйверов ОС.

Использование **стелс-алгоритмов** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо "подставляют" вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнаружения) вируса. **Полиморфик-вирусы (polymorphic)** – это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные **нестандартные приемы** часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д. Вирус может так же имитировать действия пользователя, например, по удалению антивирусной программы.

По деструктивным возможностям вирусы можно разделить на:

- **безвредные**, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- **неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске;
- **опасные вирусы**, которые могут привести к серьезным сбоям в работе компьютера;
- **очень опасные**, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить аппаратные средства компьютера.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.

Виды "вирусоподобных" программ

К "вредным программам", помимо вирусов, относятся:

- "троянские программы" (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- "intended"-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

"Троянские" программы (логические бомбы)

К "троянским" программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д. Большинство известных "троянских" программ являются программами, которые маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами "троянские" программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем. К "троянским" программам также относятся так называемые "дропперы" вирусов – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу "увидеть" заражение.

Отметим еще один тип программ (программы – "злые шутки"), которые используются для устрашения пользователя, о заражении вирусом или о каких либо предстоящих действиях с этим связанных, т. е. сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к "злым шуткам" относятся программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. К

категории "злых шуток" можно отнести также заведомо ложные сообщения о новых "супер-вирусах". Такие сообщения периодически появляются в Интернете и обычно вызывают панику среди пользователей.

Утилиты скрытого администрирования

Утилиты скрытого администрирования являются разновидностью "логических бомб" ("троянских программ"), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные "троянские" программы: отсутствие предупреждения об инсталляции и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. В результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т. п.

"Intended"- вирусы

К таким вирусам относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого

прерывания (в большинстве приводит к "зависанию" компьютера) и т.д. К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз – из "авторской" копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению. Появляются "intended"-вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

Конструкторы вирусов

К данному виду "вредных" программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т. п.

Полиморфные генераторы

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.

3. Антивирусные программы

Особенности работы антивирусных программ

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения. **Антивирусная программа** – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Вместе с тем необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При заражении компьютера вирусом очень важно своевременно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

• прекращение работы или неправильная работа ранее успешно функционировавших программ;

• медленная работа компьютера;

• невозможность загрузки операционной системы;

• исчезновение файлов и каталогов или искажение их содержимого;

• изменение даты и времени модификации файлов;

• изменение размеров файлов;

• неожиданное значительное увеличение числа файлов на диске;

• существенное уменьшение размера свободной оперативной памяти;

• вывод на экран непредусмотренных сообщений или изображений;

• подача непредусмотренных звуковых сигналов;

• частые зависания и сбои в работе компьютера.

При работе с антивирусными программами необходимо знать некоторые понятия:

Ложное срабатывание – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

Пропуск вируса – недетектирование вируса в зараженном объекте.

Сканирование по запросу – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

Сканирование налету – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.). В этом режиме антивирус постоянно активен, он присутствует в памяти "резидентно" и проверяет объекты без

Классификация антивирусных программ

По используемым технологиям антивирусной защиты:

- Классические антивирусные продукты (используют сигнатурный метод)
- Продукты проактивной антивирусной защиты. Здесь применяются технологии эвристического анализа, эмуляции кода, анализа поведения, ограничения привилегий выполнения, виртуализации рабочего окружения.
- Комбинированные решения

По видам операционных систем:

- Антивирусы для платформ Windows
- Для мобильных платформ: Android и др.
- Для платформ UNIX, Linux и т.п.

По видам защищаемых объектов:

- Рабочих станций
- Серверов (Файловых, почтовых)
- Мобильных платформ
- Систем документооборота

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, CRC-сканеры (ревизоры). Существуют также антивирусы блокировщики и иммунизаторы.

Сканеры. Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых

(неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые "маски". Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода (сигнатур), которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Во многих сканерах используются также алгоритмы "эвристического сканирования", т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории – "универсальные" и "специализированные". Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Сканеры также делятся на "резидентные" (мониторы), производящие сканирование "на лету", и "нерезидентные", обеспечивающие проверку системы только по запросу. Как правило, "резидентные" сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как "нерезидентный" сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится хранить и пополнять, и относительно небольшая скорость поиска вирусов.

CRC-сканеры. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т. д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие "анти-стелс" алгоритмы реагируют практически на 100 % вирусов сразу после появления изменений на компьютере. Характерный недостаток этих антивирусов заключается в невозможности обнаружения вируса с момента его появления и до тех пор, пока не будут произведены изменения на компьютере. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики. Антивирусные блокировщики – это резидентные программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю. К "вирусоопасным" относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и др., которые характерны для вирусов в моменты из размножения.

К достоинствам блокировщиков относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно активизируется.

Иммунизаторы. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

Обнаружение макро-вируса

Характерными проявлениями макро-вирусов являются:

- Word: невозможность конвертирования зараженного документа Word в другой формат.
- Word: зараженные файлы имеют формат Template (шаблон), поскольку при заражении Word-вирусы конвертируют файлы из формата Word Document в Template.
- Excel/Word: в STARTUP-каталоге присутствуют «чужие» файлы.

Если при проверке системы обнаружены «чужие макросы», то они могут принадлежать вирусу. Однако этот метод не работает в случае стелс-вирусов, которые запрещают работу этого пункта меню, что, в свою очередь, является достаточным основанием считать систему зараженной.

Многие вирусы имеют ошибки или некорректно работают в различных версиях Word/Excel, в результате чего Word/Excel выдают сообщения об ошибке.

Сигналом о вирусе являются и изменения в файлах и системной конфигурации Word, Excel и Windows. Многие вирусы тем или иным образом меняют пункты меню Tools/Options — разрешают или запрещают функции «Prompt to Save Normal Template», «Allow Fast Save», «Virus Protection». Некоторые вирусы устанавливают на файлы пароль при их заражении. Большое количество вирусов создает новые секции и/или опции в файле конфигурации Windows (WIN.INI).

Естественно, что к проявлениям вируса относятся такие очевидные факты, как появление сообщений или диалогов с достаточно странным содержанием или на языке, не совпадающем с языком установленной версии Word/Excel.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет

значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Антивирусная программа состоит из нескольких частей:

1. Модуль резидентной защиты.
2. Модуль карантина.
3. Модуль «протектора» антивируса.
4. Коннектор к антивирус серверу.
5. Модуль обновления.
6. Модуль сканера компьютера.

Факторы, определяющие качество антивирусных программ

Качество антивирусной программы определяется несколькими факторами. Перечислим их по степени важности:

1. Надежность и удобство работы – отсутствие "зависаний" антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.

2. Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и архивированных файлов. Отсутствие "ложных срабатываний". Возможность лечения зараженных объектов.

3. Существование версий антивируса под все популярные платформы (Windows, Linux и т. д.).

4. Возможность сканирование "налету".

5. Существование серверных версий с возможностью администрирования сети.

6. Скорость работы.

Примеры антивирусных программ:

Антивирус Касперского защищает от вредоносных программ, спама, хакерских атак, кражи личных данных и интернет-мошенничества, безопасность при работе с онлайн-банкингом, т.е. обеспечивает комплексную защиту.

Dr.Web также обеспечивает комплексную защиту. Включает следующие компоненты: антивирус, антишпион, антируткит, антиспам, веб-антивирус, брандмауэр, защищает от несанкционированного доступа, способствует предотвращению утечек важных данных, блокирует подозрительные соединения на уровне пакетов и приложений.