УДК 004.491

Нарзикулов А.Р.
студент
4 курс, факультет «Информационные системы и технологии»
Донской государственный технический университет
Россия, г. Азов
Рудов Г.А.
студент
4 курс, факультет «Информационные системы и технологии»
Донской государственный технический университет
Россия, г. Азов
Кочетков Ю.А.
студент
4 курс, факультет «Информационные системы и технологии»
Донской государственный технический университет
Россия, г. Азов

ВРЕДОНОСНЫЕ ПРОГРАММЫ И КАК ОТ НИХ ОБЕЗОПАСИТЬСЯ

Аннотация: *Статья посвящена компьютерным вирусам и способам защиты от них. В статье описываются основные существующие виды компьютерных вирусов. Рассматриваются методы антивирусной защиты и безопасный режим. Приведены интересные факты о вирусах.*

Ключевые слова: *антивирус, вирус, кибербезопасность, информация, безопасный режим.*

Annotation: *The article is about computer viruses and how to protect against them. The article describes the main existing types of computer viruses. The methods of anti-virus protection and safe mode are considered. Interesting facts about viruses.*

Key words: *antivirus, virus, cybersecurity, information, safe mode.*

Компьютерный вирус – программное обеспечение создано для того, чтобы испортить, уничтожить, похитить, либо причинить иной ущерб данным, компьютеру или сети. Вирусы распространяются посредством соединения с другими программами, документами или путём записи в сектор начальной загрузки диска. Вирусы могут наносить чрезвычайный разрушительный урон, стирая диск или повреждая программы. Ряд вирусов, чтобы начать свои разрушительные действия, ожидают запланированную дату. Имеются вирусы, задача которых является не уничтожение информации, а постепенное кодирование секторов диска, допуская доступ к кодированной информации только при наличии вируса в памяти. Чтение данной информации становится практически невозможно: вместо привычных нам наименований файлов и директорий – сплошной мусор из неразборчивых символов. Попытка же удаления подобного вируса может привести к абсолютной потере данных на диске.

Почему кибербезопасность так важна?

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, её изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний.

Реализация мер эффективной кибербезопасности в настоящее время является достаточно сложной задачей, так как сегодня существует гораздо больше устройств, чем людей, а злоумышленники становятся всё более изобретательными.

В современном «подключённом» мире программы расширенной киберзащиты служат на благо каждого пользователя. На индивидуальном уровне атака со взломом киберзащиты может привести к разнообразным последствиям, начиная с кражи личной информации и заканчивая вымогательством денег или потерей ценных данных, например, семейных фотоснимков. Все зависят от критически важной инфраструктуры: электростанций, больниц и финансовых

учреждений. Защита этих и других организаций важна для поддержания жизнедеятельности нашего общества.

Все получают пользу от исследования киберугроз, которым занимаются специалисты по киберугрозам. Например, 250 специалистов из команды Talos, изучающие новые и появляющиеся угрозы, а также стратегии кибератак, выявляют новые уязвимости, информируют общественность о важности кибербезопасности и повышают надежность инструментов с открытым программным кодом. Работа этих специалистов делает Интернет более безопасным для каждого пользователя.

Классификация вредоносных программ.

Термины “вирус” и "вредоносное ПО" часто используются взаимозаменяемо, но это не одно и то же. Хотя компьютерный вирус является разновидностью вредоносных программ, не все вредоносные программы являются компьютерными вирусами.

Самый простой способ отличить компьютерные вирусы от других видов вредоносных программ - это думать о вирусах в биологических терминах. Возьмем, к примеру, вирус гриппа. Грипп требует какого—то взаимодействия между двумя людьми. Например, рукопожатия, поцелуя или прикосновения к чему-то, к чему прикоснулся инфицированный человек. Как только вирус гриппа попадает в организм человека, он прикрепляется к здоровым клеткам человека, используя эти клетки для создания новых вирусных клеток.

Вирус - это специально написанная небольшая по размерам программа, имеющая специфический алгоритм, направленный на тиражирование копии программы, или её модификацию и выполнению действий развлекательного, пугающего или разрушительного характера.

Тем или иным способом вирусная программа попадает в компьютер и заражает его. Программа, внутри которой находится вирус, называется заражённой. Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и заражает другие программы, а также выполняет какие-либо вредоносные действия. Например, портит файлы или таблицу

размещения файлов на диске, занимает оперативную память и т.д. После того, как вирус выполнит свои действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа заражённой программы выглядит так же, как и незаражённой. Поэтому далеко не сразу пользователь узнаёт о присутствии вируса в машине.

Многие разновидности вирусов устроены так, что при запуске заражённой программы вирус остаётся в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере.

К числу наиболее характерных признаков заражения компьютера вирусами относятся следующие:

- некоторые программы внезапно перестают работать;
- быстро сокращается объём свободной памяти жёсткого диска;
- меняется указатель мыши или заставка на рабочем столе;
- замедляется работа системы;
- заблокирован диспетчер задач;
- операционная система не загружается;
- повреждаются файлы на носителях.

Червь. Черви являются в некотором роде вирусами, так как созданы на основе саморазмножающихся программ. Однако черви не могут заражать существующие файлы. Вместо этого червь поселяется в компьютер отдельным файлом и ищет уязвимости в сети или системе для дальнейшего распространения себя. Черви также могут подразделяться по способу заражения (электронная почта, мессенджеры, обмен файлами и пр.). Некоторые черви существуют в виде сохранённых на жёстком диске файлов, а некоторые поселяются лишь в оперативной памяти компьютера.

Троян. По своему действию является противоположностью вирусам и червям. Его предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности он делает то, что нужно злоумышленникам. Троянцы получили свое название от одноименного печально известного мифологического коня, так как под видом какой-либо полезной

программы или утилиты в систему проникает деструктивный элемент. Трояны не самовоспроизводятся и не распространяются сами по себе. Однако с увеличением вала информации и файлов в Интернете трояна стало довольно легко подцепить. Нынешние трояны эволюционировали до таких сложных форм, как, например, бэкдор (троян, пытающийся взять на себя администрирование компьютера) и троян-загрузчик (устанавливает на компьютер жертвы вредоносный код).

Руткит. В современном мире руткит представляет собой особую часть вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения. Это возможно благодаря тесной интеграции руткита с операционной системой. А некоторые руткиты могут начать свою работу прежде, чем загрузится операционная система. Таких называют буткитами. Однако, как бы ни развивался этот тип вредоносов.

Бэкдор (средство удалённого администрирования). Бэкдор, или RAT (remote administration tool), — это приложение, которое позволяет честному системному администратору или злобному злоумышленнику управлять вашим компьютером на расстоянии. В зависимости от функциональных особенностей конкретного бэкдора, хакер может установить и запустить на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру. Словом, брать на себя контроль за компьютером и информацией жертвы.

Загрузчик. Эта зараза является небольшой частью кода, используемой для дальнейшей загрузки и установки полной версии вредоноса. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает весь вредонос.

Анализ нескольких видов вредоносных программ.

Троян удаленного доступа (RAT) - это программа, которая позволяет удаленно и несанкционированно получить контроль над компьютером.

Она состоит из двух частей:

Первая часть - клиент. Находится на устройстве злоумышленника. Нужна чтобы управлять второй частью.

Вторая часть - сервер. Находится на устройстве жертвы. С помощью неё злоумышленник получает доступ к компьютеру жертвы.

При помощи данной программы злоумышленник может:

- Просматривать ваши действия на экране;
- Просматривать ваши файлы;
- Шифровать ваши файлы;
- Запускать ваши файлы;
- Останавливать и отключать сервисы системы;
- Следить за вами через вашу веб-камеру;
- Делать мелкие пакости. Например, воспроизводить различные звуки на вашем компьютере.

Самый известный троян удаленного доступа - “DarkComet”

Программа была разработана в 2008 году французским хакером Жаном-Пьером Лесуэром.

DarkComet отличается простым в использовании интерфейсом, позволяющим пользователям, которые практически не обладают техническими навыками, проводить хакерские атаки. Это позволяет шпионить через систему отслеживания нажатия клавиш, захват экрана и сбор пароля.

Управляющий хакер также может управлять питанием удаленного компьютера, позволяя включать, выключать, перезагружать устройство и т.д. Сетевые функции зараженного компьютера также можно использовать для использования в качестве прокси-сервера и маскировки его личности во время рейдов на других компьютерах. Проект DarkComet был заброшен создателем в 2014 году.

Как защититься от вируса RAT?

Если вы поняли, что ваш компьютер заражен трояном удаленного доступа, рекомендуем отключить компьютер от сети интернет, скопировать ваши важные

файлы на отдельный носитель и провести полное сканирование антивирусом. Однако, антивирусные программы не всегда могут помочь избавиться от данной угрозы. Против таких программ хорошо подойдут системы обнаружения вторжений (СОВ). Они анализируют компьютеры на предмет ненормального поведения.

Zip-бомба, также известная как “архив смерти” — архивный файл, который занимает довольно мало памяти, но при разархивировании заполняет всё свободное место на диске, что может вызвать серьезные проблемы в работе системы. Современные антивирусные программы могут распознать такие файлы.

Первая "Zip-бомба" появилась в 1996 году, когда один пользователь загрузил на доску объявлений в Фидо вредоносный архив, который открыл ничего не подозревающий администратор.

Майнеры.

Майнерами называются программы, которые задействуют ресурсы вычислительного устройства для генерации различных криптовалют. Иногда пользователи могут устанавливать это ПО самостоятельно, но иногда речь идет о нелегитимной их разновидности. Такие программы устанавливаются без ведома и согласия пользователя и называются скрытыми майнерами.

Как происходит скрытый майнинг? Чаще всего скрыто майнят пиратские популярные сайты: торрент-трекеры, форумы, сайты с фильмами и сериалами. Для того, чтобы начать майнить за счёт пользователя совершенно необязательно устанавливать на его компьютер троян или другую вирусную программу. Для этого достаточно ввести в код сайта специальный скрипт, который позволяет незаметно подключиться к системе гостей сайта. В принципе, обнаружить это достаточно просто. При таком вмешательстве загрузка процессора резко увеличивается практически до ста процентов. Однако, загружаемые торренты и без этого нагружают систему, что не позволяет определить майнинг.

Для того, чтобы увидеть нагрузку процессора на Windows, нужно зайти в «Диспетчер задач» (Task Manager).

Избежать скрытого майнинга можно несколькими способами:

• Установить специальное расширение, блокирующие веб-майнинг.

• Отключить JavaScript.

• Использовать надёжный антивирус.

Рекламный вирус (AdWare).

Рекламный вирус (AdWare) считается потенциально нежелательной программой (ПНП или PUP, potentially unwanted program), т.е. программой, которая устанавливается без специального разрешения пользователя. Данная программа мешает вашей работе в Интернете, показывая чрезмерный объем рекламных объявлений, всплывающие окна, баннеры, текстовые ссылки и автоматическое воспроизведение рекламных роликов. Цель рекламного ПО – получение заработка для своего разработчика за демонстрацию рекламы.

Типы рекламного ПО.

Имеется два вида рекламного ПО в зависимости от метода проникновения на ваш ПК: вместе с бесплатной или условно-бесплатной программой или через зараженные сайты.

Вместе с бесплатной или условно-бесплатной программой.

Когда вы скачиваете бесплатную или условно-бесплатную программу, зачастую они содержат встроенное рекламное ПО. Эти бесплатные программы используют рекламное ПО для финансирования разработки и дистрибуции. Этот тип рекламного ПО не имеет злого умысла, но может серьезно раздражать.

Часто рекламное ПО путают со шпионским ПО. Шпионы работают аналогичным образом, но они являются отдельной программой. Такие программы скачиваются неосознанно и они отслеживают ваши предпочтения по поиску в Интернете, чтобы можно было показывать рекламные объявления именно «под вас» и собирают прочую информацию

Через зараженный сайт.

Данный вид рекламного ПО, по сути, связан с «угоном» браузера. Заражение происходит при посещении зараженного сайта, в следствии чего

происходит несанкционированная установка рекламного ПО. Позже при просмотре других сайтов начинают активно показывать рекламные объявления.

Что делает рекламное ПО?

Вот несколько признаков того, что на вашем устройстве установлено рекламное ПО (AdWare):

- Домашняя страница браузера поменялась без вашего дозволения
- Рекламные объявления появляются там, где их не должно быть
- Ссылки веб-сайтов перенаправляют вас на непредвиденные страницы
- Ваш веб-браузер работает слишком медленно
- Без вашего разрешения появились новые тулбары, плагины или расширения
- Стали автоматически устанавливаться нежелательные программы

Опасно ли рекламное ПО (AdWare)?

Рекламное ПО (AdWare) больше раздражает, чем представляют серьезную опасность. Прослеживается непрерывная демонстрация баннеров, текстовых маркетинговых объявлений и всплывающих окон, которые возникают внутри окна браузера при сёрфинге в Интернете. Внезапно могут открываться случайные окна и закладки. Ваш компьютер начинает медленнее работать, все чаще бывают различные сбои в его работе.

Бывают также случаи, когда рекламное ПО может проводить сбор ваших данных. В этом случае производитель может продавать ваши рекламные данные, которые могут содержать вашу историю просмотра сайтов и содержать в себе ваш IP-адрес, поисковые запросы и посещённые сайты.

Антивирусные программы.

Проанализируем первый тип - по технологическим процессам антивирусной защиты:

- Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования);
- Продукты проактивной антивирусной защиты (продукты, применяющие только проактивные технологии антивирусной защиты);

- Комбинированные продукты (продукты, применяющие как классические, сигнатурные методы защиты, так и проактивные).

Сигнатурный метод детектирования.

Сигнатурный анализ – это один из методов антивирусной защиты, состоящий в раскрытии характерных идентифицирующих качеств каждого вируса и поиске вирусов при сопоставлении файлов с выявленными характеристиками.

Сигнатурный анализ. Данный способ выявления используется в первую очередь. Он основан на поиске сигнатур уже известных угроз в содержимом анализируемого объекта. Сигнатурой называется непрерывная конечная последовательность байт, которая необходима и достаточна для конкретной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что даёт возможность значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах Dr.Web составлены таким образом, что благодаря одной и той же записи можно выявлять целые классы или семейства угроз.

Проактивные технологии антивирусной защиты.

Проактивные технологии — комплекс технологий и методов, применяемых в антивирусном ПО, основной целью которых, в отличие от реактивных технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного ПО в системе. При этом проактивная защита стремится заблокировать потенциально опасную активность программы только в том случае, если эта активность представляет реальную угрозу. Основной минус проактивной защиты — блокирование легитимных программ (ложные срабатывания).

Основные антивирусные программы:

1) 360 Total Security.

360 Total Security построен по новой технологии, которая проверяет и защищает вашу систему на основе 5 лучших движков антивирусов:

— Bitdefender;

— QVMII;

— Avira;

— System Repair (системное восстановление);

— Облачный движок 360 Cloud.

Плюсы антивируса:

1. Не отнимает много ресурсов у компьютера. Работает очень быстро. Скорость проверки во многом зависит от производительности вашего компьютера.

2. Запуск проверки не вызывает никаких затруднений, особенно запуск полной проверки. Достаточно нажать большую кнопку "Проверить", на которой после проверки появится надпись "Исправить".

3. Высокая степень обнаружения вирусов. По умолчанию после установки у него включены облачный сканер, антивирусный движок QVM и модуль исправления системных проблем.

3. Встроенных инструментов много, но большинство из них, к сожалению, для премиум-версии. Из доступных стоит отметить ускорение игр, очистку реестра, очистку резервных копий системы, возможность сжатия диска для увеличения производительности, модуль дешифрования против разных вирусов-вымогателей.

Минусы антивируса: пытается блокировать ВСЁ. Даже продукты Microsoft.

2) Avast Free Antivirus.

Преимущества: прекрасная функциональность для бесплатного продукта, встроенная «песочница», продвинутое облачное сканирование, защита от руткитов и фишинга.

Недостатки: периодически раздражает предложениями приобрести платную версию.

3) Kaspersky Free.

Преимущества: мощный антивирусный сканер и сетевая защита, простой интерфейс, отличная защита от фишинга.

Недостатки: довольно медлительное сканирование, прилагаемая бесплатная версия Kaspersky Secure Connection VPN имеет ограничения по трафику.

Безопасный режим.

Безопасный режим – данный метод загрузки операционной системы, при котором загружаются самые минимальные компоненты. Даже фоновой картинки на «Рабочем столе» не будет. Безопасный режим хорош тем, что не дает загружаться приложениям, прописанным в автозагрузке. По этой причине его часто используют, когда компьютер заражен вирусами.

Интересные факты

1. CREEPER

Первый известный вирус был создан Робертом Томасом в 1971 году и получил название «CREEPER». Экспериментальная программа Томаса заразила мэйнфреймы на ARPANET. Телетайпное сообщение, показанное на экранах, гласило: «Я крипер: Поймай меня, если сможешь.»

2. Пугающая динамика

К 1990 году насчитывалось всего около 50 известных компьютерных вирусов. В конце 1990-х годов количество вирусов резко возросло до более чем 48 000. Сегодня каждый месяц появляются около 6 000 новых вирусов.

3. Melissa

В марте 1999 года вирус «Melissa» был настолько мощным, что заставил «Microsoft» и многие другие крупные компании отключить свои системы электронной почты. Почтовые сервера корпораций не работали до тех пор, пока вирус не был удален полностью.

4. Вирусы вне закона

На сегодняшний день во многих странах вирусы не считаются незаконным актом. Но в некоторых странах существуют законы о компьютерной

преступности. Например, в Германии запрещено обмениваться компьютерными вирусами вне зависимости от причины, а в Финляндии незаконным является даже написание компьютерного вируса.

5. Самый дорой вирус

Самым дорогим компьютерным вирусом всех времен стал червь MyDoom, который был запущен в январе 2004 года. Он привёл к убыткам в размере $ 38 млрд. Согласно предварительным оценкам, этот вирус заразил 25% всех электронных писем.

6. Хакерская группировка - Anonymous

Вступить в ряды одной из самых известных в мире хакерских группировок Anonymous довольно легко, но лишь немногие члены этой организации являются элитными хакерами, способными использовать недостатки безопасности в компьютерных системах и писать вирусы

7. Устройство USB Killer

USB Killer — это крошечное USB-устройство, которое при подключении к компьютеру быстро накапливает сверхвысокое напряжение и, разряжаясь, повреждает аппаратные компоненты устройства. Этим устройством воспользовался бывший студент колледжа Виншванат Акутота, он смог уничтожить более 60 компьютеров в учебном заведении.

Заключение

Несмотря на широкую распространенность антивирусных программ, с большими темпами увеличивается количество вирусов, а вместе с ними и новые способы заражения компьютера. Чтобы справиться со всеми вирусами, необходимо создавать более универсальный и качественно-новый подход к борьбе с ними, который будет включать в себя все положительные качества своих предшественников. К сожалению, на данный момент нет такой антивирусной программы, которая гарантировала бы абсолютную защиту от всех разновидностей вирусов.

Пользователю необходимо следить за тем, чтобы антивирусные программы, используемые для проверки, были самых последних версий и

получали свежие обновления баз данных. К тому же следует избегать посещения сайтов из не проверенных источников, а тем более скачивать файлы. Если у вас имеются важные файлы, которые вы боитесь потерять не лишним будет сделать резервное копирование на переносной накопитель или облако. Так вы сможете обезопасить данные, не полагаясь только на защиту вашего антивируса.

Использованные источники:

1. Брюс Денг. Практическое обратное проектирование: x86, x64, ARM, ядро Windows, инструменты реверсирования и запутывание.— Wiley, 2014 — 384 с.
2. Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors: Обнаружение и защита.— СПб.: БХВ-Петербург, 2006.— 275 с.
3. Анин Б.Ю. Защита компьютерной информации.— СПб.: БХВ-Петербург, 2000.— 384 с.
4. Хоглунд Г., Батлер Дж. Руткиты: внедрение в ядро Windows.— Питер, 2007.— 283 с.
5. Гульев И.А. Компьютерные вирусы, взгляд изнутри.— ДМК, 1998.— 306 с.
6. Мазаник С. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей.— Эксмо, 2014.— 256 с.
7. Отчет об угрозах выявляет детей дошкольного возраста, разрабатывающих вредоносный код | AVG. [Электронный ресурс]. URL: https://www.avg.com/en/signal/kids-writing-trojans-show-computer-skills-friends (дата обращения: 15.03.2020).
8. Классификация, характеристики, примеры – Компьютерные вирусы. [Электронный ресурс]. URL: https://www.sites.google.com/site/komputernyevirusysazykina/home/antivirusnye-programmy/klassifikacia (дата обращения: 16.03.2020).
7. Что такое Adware? Советы для защиты от рекламного ПО. [Электронный ресурс]. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/345985.php (дата обращения: 16.03.2020).