Муниципальное бюджетное общеобразовательное учреждение
Кубинская средняя общеобразовательная школа №2
имени Героя Советского Союза Безбородова В.П.

Индивидуальный проект

на тему:

«Вредоносные программы – классификация, отличительные признаки, методы защиты от них»

Выполнил:
ученик «11 Б» класса
Шеков Иван Евгеньевич

Руководитель:
учитель информатики
Кичкина Марина Петровна

г. Кубинка
2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

С развитием компьютерных технологий в повседневную жизнь человека пришло много новых понятий. Одними из таких стали различные наименования вредоносных ПО, виды которых я подробно рассмотрю, разобрав их функции и выяснив, в чем заключается их опасность.

Актуальность проблемы: в нынешнее время у большинства населения есть доступ к глобальной сети – Интернету, где, помимо ценной информации, неопытного пользователя часто поджидают угрозы, способные вывести его гаджет из строя. В связи с постоянным развитием информационной сферы, с каждым годом таких угроз становится все больше и они обретают все более массовый характер.

Цель проекта: рассмотреть основные типы вредоносных программ, их задачи и методы противодействия им.

Задачи проекта:

- Разобрать наиболее распространенные виды вредоносного/нежелательного ПО.
- Поведать о значении их применения.
- Рассказать о том, где и при каких обстоятельствах можно наткнуться на данные программы.
- Рассмотреть методы противодействия каждому из рассматриваемых видов вредоносных и нежелательных ПО и дать советы, направленные на предотвращение столкновения с ними.

Тип проекта:

- По доминирующей в проекте деятельности: информационный
- По количеству участников проекта: индивидуальный
- По широте охвата содержания: монопредметный

Предмет, в рамках которого выполнен проект: информатика.

Методы, используемые в работе над проектом: поиск и анализ информации по выбранной теме в общедоступных источниках Интернета.

Форма представления проекта: презентация.

Выводы: Данный проект в понятной и доступной форме ознакомит с основной информацией, касающейся вредоносных ПО.

Возможные области применения: Материалы проекта послужат для изучения выбранной темы в общих чертах.

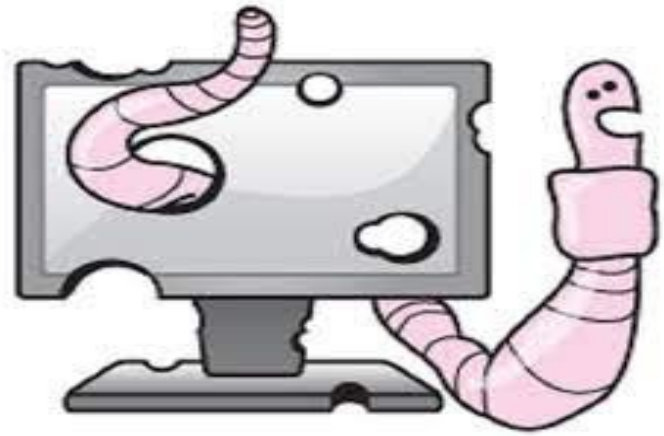
Что такое вредоносное ПО?

Вредоносное ПО – это любое программное обеспечение, которое предназначено для получения несанкционированного доступа к вычислительным ресурсам ЭВМ (электронной вычислительной машины) или к информации, хранимой на ней. Делается это с целью несанкционированного использования ресурсов ЭВМ или нанесения ущерба путём копирования, искажения, удаления или подмены информации.

Классификация вредоносного ПО

Типов вредоносных программ существует большое множество. Я рассмотрю самые основные из них, которые могут представлять опасность для рядовых пользователей.

1. Сетевые черви



Сетевые черви (network worms) – тип вредоносных программ, задача которых – распространяться по локальным сетям и интернету, при этом создавая свои многочисленные копии. Для размножения они могут использовать устройства и сетевые протоколы.

По форме существования сетевых червей можно разделить на две объемных группы: обычные черви и пакетные черви. Обычные проникают в систему через интернет или флеш-накопители, воспроизводят свои копии в большом количестве, после чего рассылают их по электронным адресам, найденным в компьютере пользователя, или распределяют их по папкам общего доступа в локальной сети. Пакетные же черви представляют собой особый сетевой пакет. После внедрения в устройство, они стараются проникнуть в оперативную память для сбора

персональных данных пользователя или какой-либо другой ценной информации.

1.1. Классификация и способы распространения червей

Основным признаком различия между данными вредоносными программами является способ распространения по удаленным компьютерам. Всего групп таких механизмов на данный момент существует две:

К первой группе относят способы, которые используют различные системные недоработки, уязвимости в ПО. К ним можно отнести:

- Репликацию через сеть: Червь находит удаленные ПК и воспроизводит себя в разных каталогах, подходящих для осуществления записи. Поиск таких каталогов осуществляется с помощью функций ОС (операционной системы).
- Репликацию через ресурсы общего пользования: Червь попадает на какой-либо сервер, изменяя расположенные на нем файлы на зараженные. После загрузки и запуска таких файлов, червь проникает в ОС.
- Репликацию через уязвимости ОС, приложений и программ: Черви ищут ОС с уязвимым ПО и по нахождению отправляют запрос для эксплуатации (использования) уязвимости.
- Паразитирование на других вредоносных программах: Червь находит на компьютере пользователя другую вредоносную программу и начинает использовать ее для своего распространения.

Вторую же группу распространения составляют различные методы социальной инженерии. Обсуждаемые вредоносные объекты, входящие в эту группу, попадают на ПК, благодаря неосторожности пользователя, который, в результате психологического манипулирования или же простой невнимательности, сам впускает червей в систему и активирует их. Представителями такой группы являются например:

- Почтовые черви (Email – Worm) – рассылаются в виде вложений к сообщениям электронной почты. Вложением может являться ссылка на файл, размещенный на вредоносном сайте, или же копия самого червя. При непосредственном переходе по ссылке или открытии файла червь проникает в систему и свои копии старается отправить по различным адресам, которые указаны в

адресной книге почтового клиента и зачастую в файлах, имеющихся на жестком диске.

- IM – черви (IM – Worm) – пользуются службами мгновенного обмена сообщениями. Во многом они схожи с почтовыми червями и по сути отличаются лишь тем, что рассылают зараженные файлы или ссылки по списку контактов в мессенджере, а не по базе почтовых адресов.
- Черви для файлообменных сетей (P2P – Worm) – распространяются через торрент – трекеры и другие подобные сервисы. Копии таких червей при попадании в систему внедряются в каталог обмена файлами под видом популярного контента.

1.2. Вред наносимый червями и способы защиты от них

Последствия работы червей могут быть весьма печальными как для ОС, так и для самого пользователя. К таковым можно отнести:

- Замедленную работу ПК
- Уменьшение места на жестком диске и объема свободной оперативной памяти (зависит от веса и количества копий червя)
- Проблемы с работой программ или приложений
- Потерю данных
- Появление системных ошибок, самопроизвольную перезагрузку, внезапное выключение

Для защиты от сетевых червей, пользователю необходимо внимательно проверять файлы, закачиваемые им в систему, а также использовать антивирусные программы (о некоторых из которых я поведаю в завершающей части своего проекта), межсетевые экраны (брандмауэры), обновленные и современные ОС, поддерживаемые компаниями – производителями.

2. Вирусы – маскировщики (Rootkit)

Вирусы – маскировщики (Rootkit) – тип вредоносных ПО, основная цель которых - предоставить злоумышленникам доступ к устройству и полный или частичный контроль над ним. Большинство руткитов влияют на работу операционной системы, а некоторые из них могут также поразить оборудование и прошивку компьютера. Отличительная черта данных вредоносных программ заключается в

намеренном скрытии их присутствия на ПК, в том числе и в период их активности.

Получив доступ к компьютерам, руткиты позволяют киберпреступникам красть личные данные пользователей, загружать другие вредоносные ПО и использовать компьютеры в DDoS-атаках (массовых заходах с различных ПК на веб-ресурсы с целью довести их до отказа путем перегрузки).

2.1. Способы проникновения руткитов в систему

Руткиты устанавливаются на ПК несколькими методами:

1. С помощью применения методов социальной инженерии (пользователи неосознанно загружают вредоносные программы).

2. Засчет использования уязвимостей ПО и ОС.

3. В связке с другими файлами, например пиратскими носителями или приложениями, скачанными из подозрительных непроверенных источников.

2.2. Виды руткитов

1) Аппаратные руткиты и руткиты для прошивки

Аппаратные руткиты и руткиты для прошивки могут влиять на работу жестких дисков, маршрутизаторов и системного BIOS (программное обеспечение, установленное на небольшой микросхеме памяти на материнской плате компьютера). Они нацелены на прошивку устройства, а не на операционную систему и предназначены для установки вредоносного ПО, которое трудно обнаружить. Руткиты влияют на поведение оборудования, позволяя злоумышленникам

записывать нажатия клавиш и отслеживать активность в Интернете. Аппаратные руткиты и руткиты для прошивки встречаются реже, чем другие типы руткитов, но представляют серьезную угрозу для сетевой безопасности.

2) Руткиты загрузчика

Механизм загрузчика отвечает за загрузку операционной системы компьютера. При атаке на систему руткит загрузчика заменяет подлинный загрузчик взломанным. Это приводит к тому, что руткит активируется до того, как операционная система компьютера полностью загрузится.

3) Руткиты памяти

Руткиты памяти скрываются в оперативной памяти компьютера и выполняют вредоносные действия в фоновом режиме, используя ресурсы компьютера. Руткиты памяти влияют на производительность оперативной памяти компьютера. Этот тип руткитов хранится только в оперативной памяти и не содержит постоянного кода, поэтому исчезает при перезагрузке системы. Однако для их полного устранения могут потребоваться дополнительные действия. Из-за короткого срока существования они не воспринимаются как серьезная угроза.

4) Руткиты приложений

Руткиты приложений заменяют стандартные файлы на компьютере файлами руткитов и даже могут изменить работу стандартных приложений. Эти руткиты могут влиять на приложения Microsoft Office и такие программы, как Notepad и Paint. Злоумышленники могут получить доступ к компьютеру при каждом запуске этих приложений. Пользователям трудно обнаружить подобные руткиты, поскольку зараженные приложения работают в обычном режиме. Однако антивирусные программы могут обнаружить руткиты, поскольку работают на прикладном уровне так же, как и они.

5) Руткиты режима ядра

Руткиты в режиме ядра представляют собой наиболее серьезную угрозу, поскольку их целью является ядро операционной системы. Злоумышленники используют такие руткиты не только для доступа к

файлам на компьютере, но и для изменения функционирования операционной системы путем добавления собственного кода.

2.3. Как избежать заражения руткитом

Чтобы предотвратить проникновение руткита в ОС, нужно следовать довольно простым правилам:

- Не подключать к компьютеру незнакомые, непроверенные устройства
- Не скачивать программы с неизвестных источников
- Не доверять различному спаму, приходящему на электронную почту
- Не заходить на подозрительные сайты

3. Вирусы – шпионы (Spyware)

Шпионские программы (spyware) - это еще один распространенный тип нежелательного программного обеспечения, предназначенного для несанкционированного сбора данных с устройства пользователя. Многие шпионские программы могут являться легальными и распространяться через официальные магазины приложений. Они используются, например, для сбора информации о местоположении устройства, посещаемых веб-сайтах, конфигурации компьютера, используемом программном обеспечении, вводимых с клавиатуры данных и т. д. Как правило, шпионские программы не имеют явно вредоносной функции (для устройства жертвы), но они могут привести к утечке конфиденциальных данных и нарушению приватности пользователя.

3.1. Классификация шпионских программ

Шпионские программы делятся на два больших типа:

1) Трекеры (программы слежения)

Трекеры (отслеживающие устройства) передают злоумышленникам такие данные, как местоположение устройства, открытые веб-сайты, документы и списки контактов. Трекеры можно разделить на два подтипа: аппаратные и программные. В рамках выбранной мною темы, стоит рассмотреть конкретно программные трекеры.

Программные трекеры используются для сбора любых данных об активности пользователя на устройстве. Они также могут быть легитимными.

К легитимным трекерам традиционно относятся всевозможные браузерные панели инструментов и целые интернет-браузеры, выпускаемые поисковыми системами и крупными интернет-порталами, такими как Yahoo, Yandex и Mail.ru. С разрешения или по незнанию пользователя такие продукты собирают исчерпывающую информацию о просмотре интернет-страниц, которая используется для разработки сервисов и таргетирования рекламы.

2) Кейлогеры (клавиатурные шпионы)

Кейлоггер - это специальная программа или устройство, которое записывает нажатия клавиш на клавиатуре устройства. Как и трекеры, кейлоггеры можно разделить на два типа: программные и аппаратные.

Программные кейлоггеры работают как приложения, поэтому каждая операционная система имеет набор таких инструментов. Многие из этих инструментов могут считывать не только нажатия обычных клавиш, но и служебные клавиши, такие как Alt и Ctrl, таким образом фиксируя команды по комбинациям клавиш. Некоторые кейлоггеры передают собранные ими данные мошенникам и другим злоумышленникам.

Аппаратные кейлоггеры - это небольшие устройства, которые подключаются к компьютеру. В отличие от программных кейлоггеров, аппаратные кейлоггеры не затрагивают жесткий диск: все данные сохраняются во внутренней памяти или на SD-карте.

3.2. Использование шпионских программ

Основная цель шпионских программ – несанкционированный сбор информации с устройств. Однако очень часто они используются для

сбора маркетинговой информации и составления профиля пользователей для целевого показа рекламы. Такая информация, как конфигурация компьютера, программное обеспечение, посещаемые веб-сайты, статистика запросов в поисковых системах и даже слова, набираемые с клавиатуры, может очень точно определить род занятий и круг интересов пользователя. В этом случае, прослеживается связка с рекламным ПО, когда шпионы собирают раннее перечисленные данные и передают их на сервера рекламных компаний. Там информация анализируется и используется для показа рекламы конкретному пользователю, иногда через неправомерное внедрение в содержимое.

3.3. Источники программ-шпионов

Источники шпионских программ можно разделить на два основных канала: первый – незаконный, мало чем отличающийся от распространения вредоносных объектов. Злоумышленники могут обманом заставить пользователей установить шпионские приложения или могут тайно внедрить их, используя незакрытые уязвимости. Второй путь – легальный: шпионские модули могут быть включены в обычное ПО или устанавливаться дополнительно к нему (без ведома пользователя во время установки). Типичным примером второй группы являются некоторые версии "фирменных" браузеров и их панели инструментов, которые на законных основаниях собирают огромное количество информации о действиях пользователя для разработчиков. То же самое касается и новых версий ОС. Например, Windows 10 стала скандальной в самом начале своего жизненного пути, когда было обнаружено, что многие ее функции собирают "телеметрию" (технологический комплекс, при помощи которого производятся удаленные измерения и сбор информации для предоставления оператору или пользователю). По мнению многих исследователей, подобные легитимные функции шпионажа, скрытые или открытые, присутствуют практически во всех современных операционных системах.

3.4. Методы защиты от шпионских программ

Чтобы защитить себя от шпионских программ, нужно выполнять ряд простых действий:

- Установить современную антивирусную программу и активировать в ней функции поиска рекламных и шпионских программ (adware и spyware).

- Установить брандмауэр и контролировать сетевую активность загруженных программ.
- Внимательно проверять настройки приватности операционных систем и браузеров, отключать лишние функции и отправку личных данных кому-либо.
- Внимательно относиться к установке приложений и выбору компонентов при инсталляции. Вместе с полезной программой вам, при невнимательности, может быть поставлен целый набор нежелательного ПО.
- Периодически просматривать список установленных программ и удалять неопознанные или редко используемые.

4. Рекламные ПО (Adware)

Рекламные программы (adware) - это тип нежелательного программного обеспечения, которое отображает рекламу на компьютере пользователя, перенаправляет поисковые запросы на рекламные сайты и собирает маркетинговую информацию. Adware собирает личные данные пользователя и передает их на сервер. После обработки информации сервер предлагает пользователю релевантную (т.е. соответствующую его интересам) рекламу.

4.1. Классификация рекламных программ

Рекламные программы можно разделить по способу их реализации: на самостоятельные приложения, запускаемые при старте системы и на модули, встраиваемые в существующие процессы.

Например, интернет-браузер может являться объектом такого встраивания.

Онлайн – adware используется в программах, для работы которых требуется подключение к Интернету. Рекламные баннеры загружаются из внешнего источника и отображаются так, что напоминают рекламу на сайте. Можно столкнуться и с образцами, которые не требуют подключения: заранее подготовленный набор баннеров хранится на диске компьютера вместе с другими программными компонентами.

Рекламная программа может распространяться как легально, так и нелегально. В первом случае разработчики получают от рекламных сетей дополнительные компоненты, которые встраиваются при создании приложения; во втором - злоумышленники распространяют такие модули по нелегальным каналам с целью получения прибыли.

4.2. Источники adware

Существует несколько способов появления на компьютере рекламных программ (adware).

Первый способ – вместе с бесплатным программным обеспечением. Показ рекламы приносит доход разработчику, который затем тратится на дальнейшее совершенствование приложения. Это вполне законный сценарий, и пользователи обычно заранее предупреждаются о наличии рекламы.

Второй способ - через зараженные веб-сайты. При посещении таких сайтов программа устанавливается без предупреждения. Хакеры используют уязвимости браузера, чтобы позволить ей проникнуть в систему. Этот тип рекламного ПО известен как Browser Hijackers.

Рекламные модули также могут быть загружены и установлены вредоносными агентами, уже присутствующими в системе, например троянскими загрузчиками.

4.3. Как избавиться от adware

Избавиться от надоедливой рекламы можно с помощью антивируса. Если программа установлена без вашего разрешения, то это — главная причина полагать, что она предоставляет опасность для ваших данных. Рекомендуется полностью удалить такой объект.

Некоторые разработчики маскируют файлы нежелательных составляющих своих приложений. В результате антивирус не распознает их как угрозу, а воспринимает как неотъемлемую часть программного обеспечения, без которой невозможна корректная работа. Для таких случаев существуют специальные инструменты, которые удаляют рекламные объявления, не нарушая работу всего программного обеспечения.

В некоторых случаях, антивирусные программы поначалу могут не обращать внимания на рекламное ПО, позволяя ему оставаться в системе в течение длительного периода времени без особых проблем. Помните, что многие антивирусы имеют функцию обнаружения adware, которая может быть отключена по умолчанию. После обнаружения нежелательные программы могут быть удалены.

5. Троянские программы (Trojan)

Троянская программа (Trojan) - это вредоносный агент, основное отличие которого от обычного вируса заключается в способе его распространения. Традиционно их называют «троянскими конями», потому что они обычно проникают в системы, маскируясь под обычные, легитимные программы. После проникновения они могут выполнять ряд действий, включая сбор информации об устройстве и его владельце, кражу данных, хранящихся на компьютере, блокировку доступа к информации пользователя, вывод из строя операционной системы и т.п.

5.1. Классификация троянов

Одним из вариантов классификации является деление на следующие типы:

- RAT (Remote Access / Administration Tool)
- Вымогатели (Ransomware)
- Шифровальщики
- Загрузчики
- Дезактиваторы систем защиты
- Банкеры
- DDoS-трояны

RAT - это троянская программа, предназначенная для шпионажа. После установки в систему она предоставляет злоумышленнику широкий спектр функций, включая запись экрана жертвы, доступ к файловой системе, запись видео с веб-камеры и звука с микрофона, кражу идентификационных файлов браузера (cookies) и установку других программ. В качестве примеров можно назвать DarkComet и AndroRAT.

Вымогатели (Ransomware) - это тип вредоносных объектов, которые блокируют доступ к системе и данным, а после угрожают пользователям удалением файлов с их компьютеров или распространением личных данных в Интернете, и требуют уплаты выкупа, чтобы избежать таких негативных последствий. Примером такого поведения является семейство WinLock.

Шифровальщики — усовершенствованная разновидность вымогателей, которая использует криптографию в качестве средства блокировки доступа. В случае с обычным "винлокером" простое удаление вредоносной программы позволит получить доступ к информации, но в данном случае уничтожение самой программы-шифровальщика ничего не даст, и зашифрованные файлы останутся недоступными. Однако с помощью антивирусного программного обеспечения, в некоторых случаях, удается восстановить данные. CryZip является одним из наиболее известных примеров шифровальщиков.

Загрузчики — вид вредоносных агентов, которые предназначены для загрузки из интернета других вредоносных программ или файлов. Пример загрузчика — Nemucode.

Дезактиваторы систем защиты — это троянские программы, удаляющие или останавливающие антивирусы, сетевые экраны и другие средства обеспечения безопасности.

Банкеры — разновидность «троянских коней», специализирующаяся на краже банковских данных (номер счета, PIN-код, CVV и т.д.).

DDoS-трояны (боты) — вредоносы, используемые хакерами для формирования ботнета (компьютерной сети, состоящей из некоторого количества хостов с запущенными ботами — автономным программным обеспечением) с целью проведения атак типа «отказ в обслуживании».

5.2. Объекты воздействия троянов

Целью таких вредоносных агентов часто являются обычные ПК и их пользователи, но возможны инциденты и в корпоративной среде. Они также могут заражать множество компьютеров через спам по электронной почте с целью формирования ботнетов. Некоторые трояны встраиваются в легитимное программное обеспечение и не мешают его функционированию. Поэтому жертва даже не подозревает об их работе в системе. Помимо персональных компьютеров, злоумышленники могут заражать и мобильные устройства, чтобы шпионить за жертвами или красть конфиденциальную информацию.

5.3. Источники троянских ПО

Возможными источниками угроз являются файлообменники и торрент-трекеры, на которые злоумышленники загружают вредоносный код под видом легальной программы, поддельные веб-сайты и спам по электронной почте. Важное правило для защиты - не переходить по подозрительным ссылкам и не запускать подозрительные программы. Большинство троянских программ успешно обнаруживаются антивирусными и антишпионскими программами.

5.4. Профилактика и избавление от троянских вирусов

Касаемо профилактики, пункты в общем-то стандартны, как и для других вредоносов. Чтобы минимизировать шанс столкновения с троянами, не стоит переходить по подозрительным ссылкам, открывать непроверенные сайты и в особенности – скачивать файлы из недоверенных источников. Если же троян все-таки попал в систему, самым простым и надежным способом избавиться от него будет использование лицензионной версии антивируса, в связи с проблематичностью ручного обнаружения и удаления этого типа вирусов самим пользователем ОС без подручных инструментов и утилит, которые ориентированы на нахождение зловредов.

Заключение

В ходе выполнения работы я рассмотрел основные типы вредоносных и нежелательных программ, с которыми наиболее часто сталкиваются рядовые пользователи. Учитывая тенденции разработок и усовершенствования компьютерных технологий, присущие последним десятилетиям, связанные с этими процессами темы с каждым днем приобретают все большее значение для общества, так как все больше людей начинают связывать себя с миром информационных технологий и все больше информации переносится на электронные носители. Соответственно, в этой сфере растет количество угроз, в частности разобранных мною в данной работе. Подытожив хочу сказать, что большинству из них можно противодействовать, особенно зная, что они из себя представляют. Поэтому я надеюсь, что поднятая мною тема будет распространяться, тем самым препятствуя злоумышленникам совершать их неправомерные деяния в отношении данных пользователей сетей.

Источники информации:

1) https://www.anti-malware.ru/
2) https://onoutbukax.ru/
3) https://www.kaspersky.ru/
4) https://ru.wikipedia.org/
5) Книга Валентина Холмогорова «PRO вирусы»