1 Понятие вредоносного по
2 Виды вредоносного ПО
2.1 Разновидности вирусов
2.2 Вирусы
2.3 Черви
2.4 Трояны
2.5 Бэкдоры
2.6 Руткиты
2.7 Боты
2.8 Шпионы
2.9 Классификация по степени опасности
2.10 Рекламный вирус
3 Деструктивные функции вредоносного ПО
3.1 Обход банковской системы двухфакторной аутентификации3.2 Пример веб-инжекта для вконтакте
3.2 Методы
3.2.1 Методы проникновения
3.2.2 Методы заражения (Стандартные методы заражения (Kasp))
3.3 Процесс заражения
3.4 Признаки заражения
3.5 Защита от заражения
4 Мифы и факты
5 Заключение
6 Полезные Ссылки

1 Понятие вредоносного по

Вредоносного по – это любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации. Многие[какие?] антивирусы считают крэки (кряки), кейгены и прочие программы для взлома приложений вредоносными программами, или потенциально опасными.

2 Виды вредоносного ПО

Поскольку киберпреступники придумывают все более сложные способы проникновения в системы пользователей, рынок вредоносных программ существенно расширился и делятся на несколько видов

2.1 Разновидности вирусов

Существует большое количество различных компьютерных вирусов. Одни из них могут просто заставлять двигаться курсор мыши, другие могут украсть ваши личные данные и даже повредить работу всей операционной системы. Давайте рассмотрим основные виды компьютерных вирусов.

2.2 Вирусы

Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях или (раньше) на дискетах. По данным Национального института стандартов и технологий (NIST) , первый компьютерный вирус под названием «Brain» был написан в 1986 году двумя братьями с целью наказать пиратов, ворующих ПО у компании. Вирус заражал загрузочный сектор дискет и передавался на другие компьютеры через скопированные зараженные

2.3 Черви

В отличие от вирусов, червям для распространения не требуются вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев. Используя уязвимости сети, например, недостатки в почтовых программах, черви могут отправлять тысячи своих копий и заражать все новые системы, и затем процесс начинается снова. Помимо того, что многие черви просто «съедают» системные ресурсы, снижая тем самым производительность компьютера, большинство из них теперь содержит вредоносные «составляющие», предназначенные для кражи или удаления файлов.

2.4 Трояны

Более известные как троянцы, эти программы маскируются под легитимные файлы или ПО. После скачивания и установки они вносят изменения в систему и осуществляют вредоносную деятельность без ведома или согласия жертвы.

2.5 Бэкдоры

Дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом

2.6 Руткиты

Руткиты — это набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), обеспечивающих:

¾ маскировку объектов (процессов, файлов, каталогов, драйверов);

¾ управление (событиями, происходящими в системе);

¾ сбор данных (параметров системы).

Термин Rootkit исторически пришёл из мира UNIX, и под этим термином понимается набор утилит или специальный модуль ядра, которые злоумышленник устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Этот набор, как правило, включает в себя разнообразные утилиты для «заметания следов» вторжения в систему, делает незаметными снифферы, сканеры, кейлоггеры, троянские программы, замещающие основные утилиты UNIX (в случае не ядерного руткита). Rootkit позволяет взломщику закрепиться во взломанной системе и скрыть следы своей деятельности путём скрытия файлов, процессов, а также самого присутствия руткита в системе.

2.7 Боты

Вредоносные программы, наделенные способностью объединяться в ботнеты

2.8 Шпионы

Вредоносное ПО, способное следить за пользователем и передавать злоумышленникам информацию, получаемую с его зараженного устройства

2.9 Классификация по степени опасности

2.10 Рекламный вирус

Одним из наиболее распространенных типов вредоносных программ является рекламное ПО. Программы автоматически доставляют рекламные объявления на хост-компьютеры. Среди разновидностей Adware - всплывающие рекламные объявления на веб-страницах и реклама, входящая в состав «бесплатного» ПО. Некоторые рекламные программы относительно безвредны, в других используются инструменты отслеживания для сбора информации о вашем местонахождении или истории посещения сайтов и вывода целевых объявлений на экран вашего компьютера. BetaNews сообщил об обнаружении нового типа рекламного ПО, который может отключить антивирусную защиту. Поскольку Adware устанавливается с согласия пользователя, такие программы нельзя назвать вредоносными: обычно они идентифицируются как «потенциально нежелательные программы»

3 Деструктивные функции вредоносного ПО

Троянские программы-блокировщики - отключают функции легитимного

ПО и выводят на экран сообщение с предложением о выкупе

• Шифровальщики - зашифровывают хранящиеся на компьютере файлы, после чего требуют у жертвы выкуп за их расшифровку. В случае отказа, могут удалить все данные либо оставить их в зашифрованном виде

• Банковские троянские программы - предназначены для кражи денег со счетов жертвы с помощью целого ряда хитроумных действий (создание удаленного доступа, изменение файлов Windows, деактивация антивирусов и так далее)

• Веб-инжекты - технология встраивания в просматриваемую пользователем веб-страницу постороннего содержимого

• Загрузчики - устанавливают на зараженное устройство другие вредоносные программы

• Майнеры - “добывают” криптовалюту на зараженном устройстве

3.1 Обход банковской системы двухфакторной аутентификации3.2 Пример веб-инжекта для вконтакте

1. В момент захода в систему “банкклиент” веб-инжект требует ввести во внедренное на веб-страницу банка окно номер мобильного телефона для продолжения работы
2. На мобильный телефон приходит СМС со ссылкой на установку банковского троянца на Android
3. Клиент вводит свои учетные данные в форму на странице банка, вся информация передается злоумышленникам
4. Мобильный троянец перехватывает СМС с одноразовым паролем от банка и пересылает его злоумышленникам

3.2 Методы

- Сменные носители информации
- Вредоносные почтовые рассылки
- Уязвимости ПО
- Социальная инженерия, фишинг
- MitM атаки

3.2.1 Методы проникновения

- Дроппер - модуль, осуществляющий извлечение содержащихся в нем модулей вируса, их распаковку и установку
- Инфектор - модуль, осуществляющий заражение файловых объектов путем изменения их внутренней структуры
- Инжектор - модуль, реализующий встраивание вредоносных компонент в процесс другого приложения
- Лоадер - модуль, осуществляющий загрузку других модулей

3.2.2 Методы заражения (Стандартные методы заражения (Kasp))

- Дроппер - модуль, осуществляющий извлечение содержащихся в нем модулей вируса, их распаковку и установку
- Инфектор - модуль, осуществляющий заражение файловых объектов путем изменения их внутренней структуры
- Инжектор - модуль, реализующий встраивание вредоносных компонент в процесс другого приложения
- Лоадер - модуль, осуществляющий загрузку других модулей

3.3 Процесс заражения

Итак, как же происходит заражение компьютерными вирусами или вредоносными программами? Существует несколько стандартных способов. Это ссылки на вредоносные сайты в электронной почте или сообщениях в социальных сетях, посещение зараженного сайта (известного как drive-by загрузка) и использование зараженного USB-накопителя на вашем компьютере. Уязвимости операционной системы и приложений позволяют злоумышленникам устанавливать вредоносное ПО на компьютеры. Поэтому для снижения риска заражения очень важно устанавливать обновления для систем безопасности, как только они становятся доступными.

Киберпреступники часто используют методы социальной инженерии, чтобы обманом заставить вас делать что-то, что угрожает вашей безопасности или безопасности вашей компании. Фишинговые сообщения являются одним из наиболее распространенных методов. Вы получаете на вид абсолютно легитимное электронное сообщение, в котором вас убеждают загрузить зараженный файл или посетить вредоносный веб-сайт. Цель хакеров - написать сообщение так, чтобы вы нашли его убедительным. Это может быть, например, предупреждение о возможном вирусном заражении или уведомление из вашего банка или сообщение от старого друга.

Конфиденциальные данные, такие как пароли, являются главной целью киберпреступников. Помимо использования вредоносных программ для перехвата паролей в момент их ввода, злоумышленники также могут собирать пароли с веб-сайтов и других компьютеров, которые они взломали. Вот почему так важно использовать уникальный и сложный пароль для каждой учетной записи. Он должен состоять из 15 и более символов, включающих буквы, цифры и специальные символы. Таким образом, если киберпреступникам удастся взломать один аккаунт, они не получат доступ ко всем вашим учетным записям. К сожалению, большинство пользователей имеют очень слабые пароли: вместо того, чтобы придумать труднодоступную комбинацию, они обращаются к standby-паролям типа «123456» или «Password123», которые преступники легко подбирают. Даже контрольные вопросы не всегда могут служить эффективной защитой, потому что многие люди дают один и тот же ответ на вопрос «Ваше любимая еда?», например, если вы находитесь в Соединенных Штатах, то почти наверняка ответ будет - «Пицца».

3.4 Признаки заражения

Хотя большинство вредоносных программ не оставляет никаких явных следов, и ваш компьютер работает нормально, иногда все же можно заметить признаки возможного заражения. Самый первый из них - снижение производительности, т.е. процессы происходят медленные, загрузка окон занимает больше времени, в фоновом режиме работают какие-то случайные программы. Еще одним настораживающим признаком может считаться измененных домашних интернет-страниц в вашем браузере или более частое, чем обычно, появление всплывающих объявлений. В некоторых случаях вредоносное ПО даже может влиять на базовые функции компьютера: не открывается Windows, нет подключения к Интернету или доступа к более высокоуровневым функциям управления системой более высокого уровня. Если вы подозреваете, что ваш компьютер может быть заражен, немедленно

произведите проверку системы. Если заражение не обнаружено, но вы все еще сомневаетесь, получите второе мнение - запустите альтернативный антивирусный сканер.

3.5 Защита от заражения

Используйте антивредоносное приложение — Установите антивредоносное приложение и регулярно обновляйте его. Это позволит защитить ваш компьютер от вирусов и других вредоносных программ. Антивредоносные приложения выполняют поиск вирусов, шпионского и другого **вредоносного** программного обеспечения, пытающегося проникнуть в вашу электронную почту, операционную систему или файлы. Новые угрозы могут появляться ежедневно, поэтому необходимо регулярно проверять наличие обновлений на веб-сайте изготовителя антивредоносного приложения.

Одновременный запуск нескольких приложений для защиты от вредоносных программ может привести к замедлению или нестабильной работе вашей системы. При установке стороннего приложения для защиты от вредоносных программ Microsoft Defender автоматически отключается. При установке двух сторонних приложений для защиты от вредоносных программ, они могут одновременно начать работу.

- **Не открывайте сообщения электронной почты от незнакомых отправителей или незнакомые вложения**. Многие вирусы передаются в виде вложений в электронные письма, и для их распространения достаточно открыть вложение. Настоятельно рекомендуем открывать только ожидаемые или известные вам вложения. Дополнительные сведения см. в следующем разделе: Защита от фишинга.
- **Используйте блокирование всплывающих окон в веб-браузере**. Всплывающие окна — это небольшие окна в браузере, отображающиеся поверх просматриваемой вами веб-страницы. Несмотря на то, что большинство таких окон используется для рекламных целей, в них может содержаться вредоносный или небезопасный код. Блокирование всплывающих окон позволяет избавиться от некоторых или даже всех всплывающих окон. Блокирование всплывающих окон в Microsoft Edge включено по умолчанию.
- **При использовании Microsoft Edge, убедитесь, что SmartScreen включен**. SmartScreen в Microsoft Edge помогает защитить от фишинга и атак вредоносных программ, предупреждая о возможной небезопасности веб-сайта или расположения загрузки. Дополнительные сведения см. в разделе Что такое фильтр SmartScreen и как он меня защищает?
- **Обратите внимание на уведомления Windows SmartScreen**. С осторожностью запускайте неизвестные приложения, скачанные из Интернета. Такие приложения с большой вероятностью могут оказаться небезопасными. Когда вы загружаете и запускаете приложение из Интернета, SmartScreen использует сведения о его репутации, чтобы предупредить вас, если приложение малоизвестно и может быть вредоносным.
- **Регулярно обновляйте Windows**. Корпорация Майкрософт регулярно выпускает особые обновления для системы безопасности, предназначенные для защиты компьютера. Обновления могут предотвратить атаки вирусов и других вредоносных программ, закрывая возможные слабые места в системе безопасности.

  Включите Центр обновления Windows, чтобы ОС Windows автоматически получала эти обновления.
- **Используйте брандмауэр**. Брандмауэр Windows или любое другое приложение брандмауэра может уведомлять вас о подозрительной активности, когда вирус или вирус-червь пытается подключиться к вашему компьютеру. Он также позволяет блокировать вирусы, червей и злоумышленников, отправляющих потенциально опасные приложения на компьютер.
- **Используйте параметры конфиденциальности браузера**. Некоторые веб-сайты могут пытаться использовать ваши личные данные для целевой рекламы, мошенничества и кражи личных сведений.

  Дополнительные сведения о настройке параметров конфиденциальности в Microsoft Edge см. в разделе Настройка параметров конфиденциальности согласно вашим потребностям.

- **Убедитесь, что функция контроля учетных записей включена**. При внесении на компьютере изменений, требующих прав администратора, функция контроля учетных записей уведомит вас об этом и предложит утвердить эти изменения. Контроль учетных записей не позволяет вирусам вносить нежелательные изменения. Чтобы открыть контроль учетных записей, проведите пальцем от правой границы экрана, а затем коснитесь элемента **Поиск**. (Если вы используете мышь, наведите указатель на правый верхний угол экрана, переместите указатель вниз, а затем щелкните **Поиск**.) Введите в поле поиска **контроль учетных записей**, а затем выберите элемент **Изменение параметров контроля учетных записей**.
- **Очистите кэш Интернета и журнал браузера** . Большинство браузеров сохраняют информацию о посещаемых веб-сайтах, а также информацию, которую вы предоставляете (например, ваше имя и адрес). Хотя хранение этих сведений на компьютере может быть полезно, существуют ситуации, когда эти сведения необходимо удалить частично или полностью, — например, если вы работаете на общедоступном компьютере и не хотите оставлять на нем свои личные сведения. Дополнительные сведения см. в статье Удаление журнала браузера.

4 Мифы и факты

Существует ряд распространенных мифов, связанных с компьютерными вирусами:

- Любое сообщение об ошибке компьютера указывает на заражение вирусом. Это неверно: сообщения об ошибках также могут быть вызваны ошибками аппаратного или программного обеспечения.
- Вирусам и червям всегда требуется взаимодействие с пользователем. Это не так. Для того чтобы вирус заразил компьютер, должен быть исполнен код, но это не требует участия пользователя. Например, сетевой червь может заражать компьютеры пользователей автоматически, если на них имеются определенные уязвимости.
- Вложения к электронным письмам от известных отправителей являются безопасными. Это не так, потому что эти вложения могут быть заражены вирусом и использоваться для распространения заражения. Даже если вы знаете отправителя, не открывайте ничего, что в чем вы не уверены.
- Антивирусные программы могут предотвратить заражение. Со своей стороны, поставщики антивирусного ПО делают все возможное, чтобы не отставать от разработчиков вредоносных программ, но пользователям обязательно следует установить на своем компьютере комплексное защитное решение класса Internet security, который включает в себя технологии, специально предназначенные для активного блокирования угроз. Даже при том, что 100-процентной защиты не существует. Нужно просто осознанно подходить к обеспечению собственной онлайн-безопасности, чтобы уменьшить риск подвергнуться атаке.
- Вирусы могут нанести физический ущерб вашему компьютеру. Что если вредоносный код приведет к перегреву компьютера или уничтожит критически важные микрочипы? Поставщики защитных решений неоднократно развенчивали этот миф - такие повреждения просто невозможны.

Между тем, рост количества устройств взаимодействующих друг с другом в Интернете Вещей (IoT), открывает дополнительные интересные возможности: что если зараженный автомобиль съедет с дороги, или зараженная «умная» печь продолжит нагреваться, пока не случится превышение нормальной нагрузки? Вредоносного ПО будущего может сделать такой физический ущерб реальностью.

У пользователей есть ряд неправильных представлений о вредоносных программах: например, многие считают, что признаки заражения всегда заметны и поэтому они смогут определить, что их компьютер заражен. Однако, как правило, вредоносное ПО не оставляет следов, и ваша система не будет показывать каких-либо признаков заражения.

Tweet: Как правило, вредоносное ПО не оставляет следов, и ваша система не будет показывать каких-либо признаков заражения. Твитни это!

Так же не стоит верить, что все сайты с хорошей репутацией безопасны. Они также могут быть взломаны киберпреступниками. А посещение зараженного вредоносным кодом легитимного сайта – еще большая вероятность для пользователя расстаться со своей личной информацией. Именно это, как пишет SecurityWeek, произошло с Всемирным банком. Также многие пользователи считают, что их личные данные - фотографии, документы и файлы - не представляют интереса для создателей вредоносных программ. Киберпреступники же используют общедоступные данные для того, чтобы атаковать отдельных пользователей, или собрать информацию, которая поможет им создать фишинговые письма, чтобы проникнуть во внутренние сети организаций.

5 Заключение

Вирусы это программы которые могут проникнуть на компьютер простого пользователя только при некорректных действия пользователя посещение сайтов паразитов или через почту. Для защиты нужно использовать антивирус.

6 Полезные Ссылки

https://youtu.be/jscrm8Mk9Zc -Как защитить ПК от вирусов

https://youtu.be/LT9Mvmj_cL0 - Как защитить компьютер от вирусов

https://youtu.be/Tnz2ZqtNdOA - Компьютерные вирусы и антивирусные программы.

https://www.lessons-tva.info/edu/e-inf1/e-inf1-4-1-3.html - Сервисное программное обеспечение ПК и основы алгоритмизации

https://studopedia.ru/18_61807_osnovnie-metodi-zashchiti-ot-kompyuternih-virusov.html - Основные методы защиты от компьютерных вирусов

https://support.microsoft.com/ru-ru/windows - Защита компьютера от вирусов