Урок-беседа на тему “Вредоносные программы” для учеников 7-10 классов

Введение 1
Классификация и виды 2
Пути заражения 8
Методы защиты от вредоносного программного обеспечения 9
Признаки заражения вредоносными программами 10
Как избавиться от вредоносной программы? 11
Итог 14

Примечание:
Жирным курсивом на зелёном фоне выделены вопросы, которые учитель может задавать классу

Текст на голубом фоне – информация для учителя

Введение

Ребята, добрый день. Сегодня хотелось бы поговорить с вами о такой важной проблеме как вредоносное ПО. Сейчас, как полагаю, все из вас являются активными пользователями ПК.

“Скажите пожалуйста, как вы понимаете термин «вредоносное ПО»? Что это значит для вас?”

Термин «вредоносное ПО» – это сокращение термина «вредоносное программное обеспечение». Вредоносные программы – это программы, намеренно разработанные и внедряемые для нанесения ущерба компьютерам и компьютерным системам.

“Зачем нам знать об этой теме?”

“Как вы думаете, кто и зачем распространяет ВПО?”

Вредоносное ПО распространяют киберпреступники. Такие программы обманывают пользователей и мешают нормальной работе с устройствами. Как только киберпреступник получает доступ к вашему устройству с помощью одного или нескольких различных методов, он использует ситуацию в своих интересах, чтобы проводить дополнительные атаки, получить учетные данные, собирать вашу личную информацию для продажи или других целей,

“Сталкивались ли вы когда-нибудь с такой проблемой? Или, может, ваши знакомые были жертвами киберпреступников?”

Да, это действительно очень печально, что в нашем обществе существуют такая проблема. Но от зла не избавишься, остаётся только искать пути защиты от него.

И сегодня я помогу вам разобраться в мире киберугроз.
Мы рассмотрим виды вредоносных программ.
Узнаем, как можно заразиться и что стоит сделать, чтобы обезопасить себя.
Также рассмотрим признаки, по которым можно понять, что ПК заражён и узнаем, что делать если вы уже заразились.

Классификация и виды вредоносных программ

В настоящий момент в мире отсутствует какая-либо общепринятая единая система классификации вредоносных программ: каждая антивирусная компания использует собственный метод их наименования и классификации.

Более распространенной и логически правильной классификацией вредоносных программ является их распределение по типам и подклассам согласно формальным признакам, определяющим их вредоносные функции. Рассмотрим основные виды вредоносных программ по их вредоносному функционалу, архитектурным особенностям и практическому назначению, а также перечислим их основные характерные признаки.

Вирусы

Сегодня существует огромное количество различных вредоносных программ, однако большинство пользователей отчего-то традиционно называет все их «вирусами». Это в корне неправильно.

“Какой функцией обладают вирусы с точки зрения биологии? А как это можно спроецировать на нашу тему?”

Чтобы отнести вредоносную программу к категории *компьютерных вирусов,* она должна отвечать критерию:

- способность заражения файловых объектов.

Под заражением понимается технология, с использованием которой вирус внедряется непосредственно в файл исполняемого приложения (программы), не нарушая при этом ее основных функциональных возможностей. Запуская такую программу на исполнение, пользователь одновременно запускает и встроенный в нее вирус, который, загрузившись в память инфицированного компьютера, реализует заложенные в него создателями деструктивные функции. Таким образом, распространение вируса происходит в том числе вместе с зараженными программами, в которые успел встроиться вирус.

Вирусы можно использовать для кражи информации, нанесения вреда компьютерам и сетям, кражи денег, отображения рекламы и многого другого.

Черви

“Предположите, как функционирует червь, опираясь на его название?”

Компьютерные черви — разновидность вредоносных компьютерных программ, обладающих способностью к саморепликации, то есть к автоматическому распространению без участия пользователя — по локальной сети, по каналам электронной почты, с использованием сменных носителей информации или иными методами. При этом считается, что большинство червей не способно заражать файловые объекты, хотя из данного правила имеются некоторые исключения.

Довольно широко распространены так называемые *почтовые черви* — эти вредоносные программы, запустившись на исполнение, отыскивают все хранящиеся на зараженном компьютере адреса электронной почты **(*“Где они их берут?”*)** (некоторые сканируют для этих целей не только адресные книги почтовых клиентов, но также различные текстовые документы, локально хранящиеся на диске и документы Office), после чего рассылают свою копию по этим адресам в виде вложения в электронное письмо. Адрес отправителя такие вредоносные программы также зачастую заимствуют из списка контактов на зараженной машине. В этом отношении нельзя не отметить, что получатель подобного сообщения, увидев послание, якобы отправленное знакомым ему человеком, с большой долей вероятности попытается открыть такое письмо и в результате сам станет очередной жертвой почтового червя.

Многие черви распространяются, копируя себя на съемные носители информации. Например, некоторые вредоносные программы данного типа размещают в корневой папке съемного накопителя (флэшки или карты памяти) файл *autorun. inf*, обеспечивающий автоматический запуск червя при каждом обращении к инфицированному накопителю. Другие черви перемещают все содержимое съемного носителя информации в скрытую папку, а вместо него размещают собственные копии или ярлыки с прежними именами папок и файлов. В результате пользователь, щелкнув мышью на значке такого файлового объекта или ярлыка, вместо открытия нужной ему папки или файла запустит на выполнение вредоносную программу.

“Как вы поняли основное отличие червя от вируса?”

В отличие от вируса, червь имеет свойство воспроизводить себя в компьютере, не требуя каких-либо действий пользователей. Еще одной особенностью компьютерного червя является то, что он распространяется не только по всей области вашего компьютера, но и автоматически рассылает свои копии по сети.

“Какой урон может наносить червь? Как он будет влиять на пропускную способность сети?”

Вы зададите вопрос, а зачем кому-нибудь нужно разрабатывать подобные программы? Прежде всего, потому что при помощи червей можно сделать сбой в системах и сетях, так как они потребляют большой объем оперативной памяти и забивают пропускную способность сетей. Червь пошлет свои копии всем вашим контактам, и далее будет распространяться в геометрической прогрессии. Компьютерные черви также могут содержать «полезные данные», которые повреждают компьютеры. Полезные нагрузки — это фрагменты кода, написанные для выполнения действий на пораженных компьютерах, помимо простого распространения червя. Полезные нагрузки обычно предназначены для кражи данных, удаления файлов или создания ботнетов.

Трояны

“Знаете ли вы, откуда пошло название?” Из Илиады: Неприступную крепость Трои удалось взять с помощью военной хитрости. Царь Итаки, Одиссей, придумал спрятать внутри деревянного коня ахейских воинов, а коня оставили перед воротами города. Троянцы решили, что греки капитулировали и в знак примирения оставили коня. Его втащили в город, а ночью греки выбрались наружу, открыли ворота и сожгли Трою. Так с помощью хитрости Одиссея закончилась Троянская война.

“Как аналогия с троянским конём описывает работу компьютерного трояна?”

Это самый многочисленный и распространенный тип вредоносных программ. В отличие от вирусов и червей, троян не способен ни к саморепликации, ни к заражению файловых объектов. Троян маскируется под обычный файл или программу и долгое время (как правило, либо до момента обнаружения, либо до переустановки операционной системы) выполняет свои функции.

Троянские программы жертва запускает на своем компьютере самостоятельно, при этом злоумышленники заставляют ее сделать это различными способами: массово рассылают троянцев в виде вложений в сообщения электронной почты под видом коммерческих предложений, сообщений почтовых служб и интернет-магазинов, скидочных купонов, бухгалтерских документов — счетов или, различных договоров. Кроме того, очагами распространения троянских программ традиционно являются сайты категории «для взрослых», всевозможные коллекции пиратских и взломанных коммерческих программ, файлообменные интернет-ресурсы, сборники утилит для взлома лицензионных продуктов (всевозможные «кряки», «кейгены» и т. д.). Шанс получить вместе со «взломанной» программой или игрой бесплатный «подарок» в виде опасного троянца намного выше, чем в случае загрузки этого же приложения с сайта разработчиков или покупки такой программы у официальных издателей.

(“Пользуетесь ли вы взломанными программами?”)

Троянец может предоставить злоумышленнику удаленный доступ к зараженному компьютеру. Как только хакер получает доступ к зараженному компьютеру, он может украсть данные (логины, финансовые данные, даже электронные деньги), установить больше вредоносных программ, изменить файлы, контролировать активность пользователей (просмотр экрана, ведение кейлогеров и т.д), а также включить компьютер в ботнет.

(“Подытожьте, пожалуйста, основные свойства каждого из трёх рассмотренных нами видов”)

Это были самые основные виды. На самом деле их существует много. Посмотрите пожалуйста на слайд и скажите о каких вы хотели бы узнать? Какое название вас привлекает?

Для учителя: на слайде будет список различных видов ВПО. Кликнув мышью по названию, вы попадёте на слайд с информацией о конкретном (который попросили ребята).

В углу всех слайдов, рассказывающих о видах, присутствует кнопка “Вернуться”. Она перенесёт вас на слайд со списком ВПО. Кнопка “далее” перенесёт вас на следующую тему “Пути заражения”.

Бэкдоры

“Как переводится бэкдор? Почему его называют чёрным ходом?”

Backdoor переводится с английского как чёрный ход. Представьте, что компьютер — это здание. Пользователь входит с главного входа, а злоумышленник с черного.

Backdoor предоставляет злоумышленникам возможность удалённого управления зараженными компьютерами. Заразив компьютер, злоумышленники могут удалённо выполнять на нем любые действия, включая отправку, получение, открытие и удаление

файлов, отображение данных и перезагрузку. В зависимости от функциональных особенностей конкретного бэкдора, взломщик может устанавливать и запускать на компьютере жертвы любое программное обеспечение, загружать и сохранять любые файлы, включать микрофон или камеру. Бэкдоры часто используются для объединения группы компьютеров-жертв в ботнет (зомби-сеть) для использования в криминальных целях.

Так же появляется возможность использовать зараженный компьютер в качестве промежуточного звена в процессе интернет-атаки на банк или какой-нибудь другой сервер: в ходе последующего расследования служба безопасности или полиция могут выйти на владельца инфицированного устройства благодаря оставленным в сети следам, а настоящие преступники останутся анонимными.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. ***(“Но что же их отличает?”)*** Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как черви), а только по специальной команде разработчика.

Шпионские программы

Шпионское программное обеспечение (spyware) чрезвычайно широко распространено. Предназначение таких программ вполне очевидно: они способны следить за пользователем и передавать злоумышленникам информацию, получаемую с его устройства.

Один из наиболее популярных типов программ-шпионов — это ***кейлоггеры*** **(“Как вы думаете, что они делают?”)**, то есть приложения, считывающие и сохраняющие в специальный журнал коды нажимаемых пользователем клавиш, а потом передающие эту информацию злоумышленникам. Таким образом, можно, например, похищать вводимые жертвой в различные экранные формы логины и пароли, а также любую иную набираемую на клавиатуре информацию.

Другие шпионы могут создавать и отправлять киберпреступникам *скриншоты* — снимки содержимого экрана зараженного компьютера, осуществлять скрытую съемку с использованием встроенной видеокамеры устройства. Кроме того, программы-шпионы, ориентированные на мобильную операционную систему Android, могут транслировать злоумышленникам географические GPS-координаты текущего положения зараженного устройства, передавать журнал звонков, фотографии, выполнять несанкционированную фото- и видеосъемку, записывать телефонные разговоры и даже использовать встроенный микрофон мобильного устройства для скрытой диктофонной записи с последующей передачей полученных звуковых файлов на удаленный управляющий сервер.

Буткиты

Буткиты (от англ. boot — «загрузка» и kit — «инструмент»), — это программы, способные заражать загрузочную запись на диске компьютера, благодаря чему запускаются либо раньше операционной системы, либо одновременно с ней, но в любом случае перед загрузкой основных средств антивирусной защиты. Из этого логически вытекает основная сложность борьбы с буткитами — поскольку они стартуют еще на раннем этапе загрузки компьютера, буткиты перехватывают некоторые функции управления операционной системой **(Какая опасность из этого вытекает?)** и, как следствие, могут парализовать запуск и нормальную работу антивирусных программ, а также блокировать попытки «вылечить»

инфицированное устройство. При неудачном удалении такой угрозы может произойти повреждение логической структуры диска, благодаря чему система и вовсе перестанет загружаться.

В общем случае алгоритм действия буткита таков: запустившись на инфицированном компьютере, он размещает свою копию в одной из свободных логических областей диска, а затем модифицирует существующую загрузочную запись, внедряя в нее собственный код, который получает управление при запуске операционной системы и загружает в оперативную память основное тело буткита. По окончании этого процесса буткит передает управление дальнейшей загрузкой оригинальной загрузочной записи, позволяя ОС стартовать в штатном режиме. На момент завершения загрузки операционной системы вредоносная программа уже находится в памяти и может выполнять различные деструктивные действия, например, перехватывать те или иные системные функции и предотвращать запуск антивирусных программ, а также блокировать пользователю доступ к сайтам их разработчиков.

Особая опасность буткитов заключается еще и в том, что, запускаясь вместе с операционной системой, эти вредоносные программы могут получить в ней максимальные привилегии (например, полномочия администратора), даже если текущий сеанс открыт пользователем с ограниченными системными правами. Таким образом, буткит имеет на зараженном компьютере поистине неограниченные возможности для реализации всевозможных вредоносных функций, включая полный доступ к файловой системе, компонентам ОС, и памяти.

Шифровальщики

Шифровальщики — это тип вредоносных программ, которые блокируют доступ пользователей к компьютерным системам и файлам, предоставляя злоумышленникам контроль над любой персональной информацией, хранящейся на устройствах жертв.

После успешного захвата контроля над компьютером жертвы злоумышленники начинают шифровать некоторые или все файлы пользователя.

В конце процесса злоумышленник отправляет жертве сообщение с объяснением того, что их файлы теперь взломаны и зашифрованы, и они могут быть расшифрованы только в том случае, если будет выплачен выкуп. ***(“В каком виде требуется выкуп?”)*** Выкуп чаще всего сейчас запрашивается в виде не отслеживаемого биткоин-платежа, который должен быть выплачен злоумышленнику.

Программы-шифровальщики
Злоумышленник зашифровывает важные данные или файлы. Жертвы лишаются доступа к ним до тех пор, пока не заплатят выкуп.

Программы-блокировщики
Программа-шантажист с функциями блокировки не позволяет пользователю войти на свое устройство и блокирует его. Жертва видит на экране сообщение о блокировке с требованием заплатить выкуп для восстановления доступа и соответствующими инструкциями. Такие

программы-шантажисты обычно не шифруют данные, поэтому при восстановлении доступа к устройству важные файлы и сведения сохраняются.

Как думаете, стоит ли выплачивать выкуп?

Выплата выкупа в данном случае не является гарантией того, что вы получите свои файлы обратно. Злоумышленник может не отправить ключ для расшифровки, или просто потерять его.

FakeAV

На какое известное нам слово наталкивает это название? Программы типа FakeAV имитируют работу антивирусного программного обеспечения. С их помощью злоумышленники пытаются вымогать у пользователя деньги в обмен на обещание обнаружения и удаления несуществующих угроз, о которых они ему сообщают.

DDoS и Dos

"Вы, вероятно, знакомы с этим термином. Расскажите, что вы знаете?" Вредоносная программа, предназначенная для проведения несанкционированной пользователем DoS- (англ. Denial of Service - отказ в обслуживании) атаки с пораженного компьютера на компьютер-жертвы по заранее определенному адресу.

При такой атаке с заражённых компьютеров системе с определенным адресом отправляется большое количество запросов, что может вызвать ее перегрузку и привести к отказу в обслуживании запросов реальных посетителей.

Для проведения успешной DDoS(англ. Distributed Denial of Service) – распределённый отказ в обслуживании)-атаки злоумышленники предварительно заражают программами данного типа множество компьютеров (например, в ходе массированной спам-рассылки), создавая ботнет. Ботнетом здесь называют сеть зараженных устройств, дистанционно управляемых злоумышленниками, например, с использованием одного или нескольких командных серверов, и умеющих обмениваться информацией. после чего каждый из заражённых компьютеров атакует заданную жертву.

"Закрепим. Чем DoS отличается от DDoS?" (ответ: при DoS атаке запросы отправляются только с одного компьютера, а при DDoS с сети компьютеров)

Майнеры

Майнер — это вредоносная программа, основной целью которой является добыча криптовалюты с использованием ресурсов компьютера жертвы. Такие вредоносные программы работают скрытно и имеют низкую вероятность обнаружения антивирусными программами.

Несмотря на то, что майнеры не занимаются кражей информации и паролей, вред от них довольно масштабен. Для эффективной добычи криптовалюты компьютеру необходимо задействовать как можно больше мощности, поэтому майнер одновременно добывает валюту на процессоре и видеокарте, а также с помощью накопителя. И даже непродолжительная работа системы в таком режиме может привести к перегреву компьютера или выходу комплектующих из строя.

Многие современные вредоносные программы являются многофункциональными и обладают формальными признаками сразу нескольких классов. Например, образец может быть наделен способностью заражать файловые объекты (признак файлового вируса), но при этом может распространяться, создавая свои копии в общедоступных сетевых папках (признак сетевого червя), а также умеет выполнять поступающие от злоумышленников команды (признак бэкдора).

Пути заражения

“Некоторые пути заражения вредоносным ПО были упомянуты ранее, какие вы помните?

Какие вы знаете помимо тех?”

(параллельно учитель может чертить схему и наносить на неё ответы ребят. Затем учитель открывает слайд и рассказывает о тех, которые не назвали)

Пример схемы см. на рис. 1

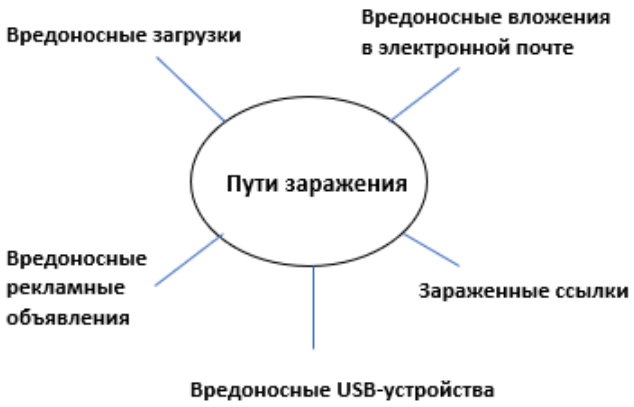

Рис. 1

Вредоносные вложения в электронной почте

Один из самых распространенных способов распространения ВПО – это отправка электронных писем с вредоносными вложениями. Злоумышленники могут маскировать эти вложения под обычные файлы, такие как документы, изображения или архивы. Когда пользователь открывает вложение, ВПО может быть запущено на его компьютере без его согласия или даже без его знания.

Зараженные ссылки

Злоумышленники могут размещать зараженные ссылки на веб-сайтах, в социальных сетях, форумах или в электронных сообщениях. Когда пользователь нажимает на такую ссылку, он может быть перенаправлен на веб-страницу, которая содержит ВПО. Иногда пользователь может быть обманут и убежден, что он переходит на легитимный сайт, в то время как на самом деле он заражает свой компьютер.

Вредоносные загрузки

Злоумышленники могут создавать вредоносные программы и размещать их на веб-сайтах или файлообменных платформах в виде обычных загрузок. Пользователи могут случайно скачать и установить эти программы, не подозревая о наличии ВПО. Вредоносные загрузки могут быть маскированы под популярные программы или игры, чтобы привлечь больше пользователей. Чаще всего их можно встретить на форумах с пиратским контентом.

Вредоносные рекламные объявления

Злоумышленники могут размещать вредоносные рекламные объявления на веб-сайтах или в приложениях. Когда пользователь нажимает на такую рекламу, он может быть перенаправлен на веб-страницу, которая содержит ВПО. Иногда реклама может содержать скрытый код, который автоматически запускает ВПО без ведома пользователя.

Вредоносные USB-устройства

Злоумышленники могут физически распространять ВПО, используя зараженные USB-устройства, такие как флеш-накопители или внешние жесткие диски. Когда пользователь подключает такое устройство к своему компьютеру, ВПО может быть автоматически запущено и начнет заражать систему.

Методы защиты от вредоносного программного обеспечения

“Как же защитить себя?” **(учитель может рисовать схему, пример схемы см. на рис. 1)**

Прежде всего, нужно быть аккуратным при работе с электронной почтой, нажатии на ссылки, скачивании файлов и подключении внешних устройств к компьютеру. Желательно не открывать вложения в почте, если они пришли от незнакомого отправителя. Также следует избегать скачивания файлов с ненадежных и непроверенных источников и не подключать к своему компьютеру неизвестные USB-флешки, не вставлять неизвестные диски.

Осторожность при посещении веб-сайтов

Следует быть осторожным при посещении веб-сайтов, особенно если они выглядят подозрительно или предлагают скачать ненадежное программное обеспечение. Также рекомендуется использовать надежные браузеры и включить функцию блокировки вредоносных сайтов.

Если вы все-таки хотите скачать программу или приложение с неизвестного сайта, проверяйте, сколько раз они были загружены. Чем больше число загрузок, тем лучше. Так же обязательно читайте отзывы.

Установка антивирусного программного обеспечения

Одним из основных методов защиты от вредоносного программного обеспечения является установка и регулярное обновление антивирусного программного обеспечения. Антивирусные программы сканируют систему на наличие вредоносных программ и блокируют их действие. Они также могут предупреждать о потенциально опасных сайтах и файловых вложениях.

Обновление программ и операционной системы

“Как обновление поможет?”

Вредоносное программное обеспечение может использовать уязвимости в программном обеспечении и операционной системе для проникновения в систему. Поэтому важно регулярно обновлять все программы и операционную систему до последних версий, чтобы исправить известные уязвимости и улучшить безопасность системы.

Регулярное создание резервных копий данных

“Зачем?”

В случае атаки вредоносного программного обеспечения, может потребоваться восстановление данных. Поэтому регулярное создание резервных копий данных является важным методом защиты. Резервные копии могут быть созданы на внешних носителях, в облачном хранилище или на других компьютерах.

Использование брандмауэра

Брандмауэр – это программное или аппаратное устройство, которое контролирует и фильтрует сетевой трафик, блокируя нежелательные соединения и защищая систему от внешних атак. Включение и настройка брандмауэра может помочь предотвратить проникновение вредоносного программного обеспечения.

Признаки заражения вредоносными программами

“Какие сразу приходят вам в голову?” (учитель может рисовать схему, пример схемы см. на рис. 1)

Если вдруг с вами случилось несчастье подхватить вредоносное ПО, важно вовремя это заметить. Иногда это поможет сохранить данные, работоспособность компьютера и вашу конфиденциальность. Чем быстрее вы это заметите, тем лучше. Хотя большинство вредоносных программ не оставляет никаких явных следов, и ваш компьютер работает нормально, иногда все же можно заметить признаки возможного заражения.

- Медленная работа, сбои и зависание компьютера. Вас должно насторожить, если ваш компьютер стал тормозить. Если задачи выполняются дольше, чем обычно, то, возможно, ваш компьютер заражен.
- Печально известный «синий экран смерти», который представляет собой сообщение о критическом сбое в операционной системе Microsoft Windows.
- Будьте внимательны при появлении на компьютере подозрительных приложений или программ, о которых вы ничего не знаете. Если вы заметили, что на компьютере появилось приложение или программа, которую вы не скачивали, будьте осторожны.
- Еще один признак возможного заражения– это странности в работе приложений или программ. Если программы стали завершаться аварийно по непонятной причине, то, возможно, ваш ПК заражён.
- изменение домашних интернет-страниц в вашем браузере или более частое, чем обычно, появление всплывающих объявлений.
- Отсутствие места для хранения.
- Отправка электронных писем и сообщений без вашего ведома.

“Какой из видов может этим заниматься?”

- 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.
- И наконец, зараженный компьютер может начать перегреваться.

Как избавиться от вредоносной программы?

“Как бы вы поступили в данной ситуации?”

(Учитель называет шаги и спрашивает у ребят, зачем нужно то или иное действие)

Ниже перечислены рекомендованные от лаборатории Касперского шаги, выполнив которые можно вручную удалить вредоносные программы с компьютеров.

Шаг 1. Отключитесь от интернета

При отключении от интернета прекращается передача данных на сервер вредоносных программ, что позволяет защитить от заражения другие устройства. Если требуется подключиться к интернету для загрузки какого-либо инструмента, отключитесь сразу после его загрузки.

Шаг 2: Перейдите в безопасный режим работы операционной системы

«Безопасный режим» позволяет запустить устройство без сторонних приложений. В этом режиме работают только стандартные программы. Он позволит изолировать проблемы на устройстве.

- Перезагрузите компьютер
- При появлении экрана входа в систему, удерживайте нажатой клавишу Shift и выберите «Питание», а затем «Перезагрузить» (шаги могут отличаться в разных версиях ОС)
- После перезагрузки компьютера выберите «Поиск и устранение неисправностей», затем «Дополнительные параметры», а затем на экране «Выбор действия» нажмите «Параметры загрузки»
- В следующем окне нажмите на кнопку «Перезагрузить» и дождитесь появления следующего экрана
- При отображении меню с нумерованными параметрами запуска, выберите номер 4 или F4, чтобы запустить компьютер в безопасном режиме

Шаг 3. Не входите в учетные записи

Цель многих вредоносных программ – получение доступа к конфиденциальной информации обычно посредством кражи учетных данных, например, в результате отслеживания нажатий клавиш или считывания пароля с экрана или из буфера обмена. Избегайте входа в учетные записи, чтобы предотвратить потерю учетных данных, не вводите логины и пароли на сайтах и в приложениях.

Шаг 4. Удалите временные файлы

Вредоносные программы могут устанавливать на устройства временные файлы, которые необходимо удалить.

- Откройте «Настройки»
- Выберите пункт «Система»
- Выберите «Хранилище»

- В разделе «Локальный диск» выберите пункт «Временные файлы»
- Выберите временные файлы, которые требуется удалить
- Нажмите на кнопку «Удалить файлы»

Шаг 5. Проверьте монитор активности

Если есть подозрение, что было установлено подозрительное обновление или приложение, закройте это приложение, если оно запущено. Монитор активности показывает запущенные на компьютере процессы и позволяет отслеживать их влияние на активность и производительность компьютера.

- В поле «Введите данные для поиска» в нижней части экрана введите «Монитор ресурсов»
- Откроется экран, показывающий действия, выполняемые на вашем устройстве
- Чтобы завершить задачу, щелкните по ней правой клавишей мыши и выберите «Завершить процесс»

Шаг 6. Запустите поиск вредоносных программ

Средства поиска вредоносных программ позволяют удалить многие распространенные инфекции. Однако если на компьютере уже установлен и используется антивирус, рекомендуется использовать другой, поскольку текущее антивирусное решение может не обнаруживать эти вредоносные программы.

Шаг 7. Проверьте браузер

Вредоносные программы часто изменяют домашнюю страницу браузера, чтобы заразить компьютер повторно. Проверьте домашнюю страницу браузера и параметры подключения, нет ли там сторонних расширений.

Как удалить вредоносные программы с Mac-устройства?

Шаг 1. Отключитесь от интернета
Шаг 2: Перейдите в безопасный режим

Переход в безопасный режим позволит изолировать проблемы на устройстве. Чтобы перейти в безопасный режим на Mac:

- Запустите Mac и сразу же нажмите и удерживайте клавишу Shift
- Отпустите клавишу Shift, как только появится окно входа в систему

Шаг 3. Не входите в учетные записи
Шаг 4. Удалите временные файлы

Вредоносные программы могут устанавливать на устройства временные файлы, которые необходимо удалить.

- Закройте все активные приложения.
- Откройте Finder, в меню нажмите «Перейти» –> «Перейти к папке», а затем введите « ~/Library/Caches/»

- Выделите временные файлы, которые требуется удалить, и переместите выбранные файлы в корзину
- Очистите корзину

Шаг 5. Проверьте монитор активности

Монитор активности показывает запущенные на компьютере процессы и позволяет отслеживать их влияние на активность и производительность компьютера. Чтобы проверить монитор активности на Mac:

- Перейдите в Finder и выберите пункт «Приложения»
- Выберите «Утилиты»
- Перейдите к монитору активности

Данные, отображаемые монитором активности, позволяют выявить подозрительные приложения в области процессов. На закладке ЦП можно также выяснить, какие приложения используют большую вычислительную мощность. При обнаружении подозрительных приложений закройте их с помощью монитора, а затем удалите из меню Finder.

Шаг 6. Запустите поиск вредоносных программ

Обычно средств поиска вредоносных программ достаточно, чтобы избавиться от большинства стандартных инфекций. Однако если на устройстве уже установлен антивирус, необходимо загрузить средство поиска вредоносных программ по запросу, отличное от используемого антивирусом. Загрузите средство поиска вредоносных программ из надежного источника, запустите его и установите программное решение безопасности, постоянно работающее в фоновом режиме и обеспечивающее защиту от существующих и возникающих угроз безопасности.

Шаг 7. Проверьте установленные расширения браузера
Шаг 8. Проверьте наличие вредоносных программ в элементах входа в систему на Mac

Элементы входа в систему включают приложения, которые запускаются при каждом запуске операционной системы. Иногда эти приложения необходимы для запуска операционной системы, а иногда они являются бесполезными и могут содержать вредоносные программы. Важно проверить элементы входа в систему и отключить те, которые могут скрывать вредоносные программы.

Для этого:

- Нажмите на логотип Apple в строке меню
- Выберите «Системные настройки», а затем – «Пользователи и группы»
- Нажмите на значок замка в левом нижнем углу
- Откройте «Элементы входа»
- Отключите неиспользуемые элементы

Шаг 9. Удалите подозрительные приложения

Изучите все установленные приложения и выясните, есть ли сред них те, которые вы никогда не используете. После этого проанализируйте каждое приложение, чтобы узнать, как оно используется. В большинстве случаев при поиске в Google удается выяснить, является ли приложение полезным или скрывает вредоносные программы. Если приложение доступно в официальном магазине приложений App Store, оно должно быть надежным. В противном случае, если приложение трудно найти у него плохие отзывы, оно может являться источником вредоносных программ.

Дополнительные инструкции по удалению вредоносного по со своего ПК можно найти в службе поддержки вашей ОС. Так же в интернете есть достаточно инструкций, которые могут помочь.

Если вы чувствуете, что не обладаете достаточными знаниями компьютера и системы, что бы разобраться в этих инструкциях, понять их логику и действительно ли они могут помочь боитесь навредить пк ещё больше, следует обратиться к специалисту.

Список надёжных антивирусов: Kaspersky Total Security, Dr.Web Security Space, McAfee LiveSafe

Mac: Avira, Norton 360, TotalAV

/По версии проекта “выбор экспертов”[1]

Итог

Подводя итог, хочется сказать, что человечество, как это не раз доказывалось, способно создавать весьма изощренные решения, особенно когда дело касается создания чего-нибудь наносящего вред другим людям. В том числе, это справедливо и для сферы IT/

Надеюсь, этот урок был вам полезен и теперь вы имеете базовое представление о том, что такое вредоносное ПО, насколько оно многообразно и как от него защититься.

В конце презентации ребят ждёт небольшой тест на закрепление материала

[1] https://www.kp.ru/expert/o-proekte/?ysclid=luhf0ffm9i6243584