Защита от вредоносного программного обеспечения (ПО)

Всё о вредоносном ПО

Как Вы знаете, каждый год проходит медицинская кампания в поддержку вакцинации против гриппа. Это делается потому, что вспышки гриппа обычно имеют сезонный характер – заболевание даёт о себе знать в определённое время года, и начинает распространяться, поражая всё больше людей.

Активность вирусов, которые атакуют ПК, смартфоны, планшетные устройства и компьютерные сети предприятий, не зависит от сезона, и её невозможно предсказать. Эпидемия «компьютерного гриппа» никогда не заканчивается. Да, из-за неё пользователи не страдают от озноба или болей во всем теле, но им не дают покоя симптомы, вызванные напастью иного рода – вредоносным ПО.

Вредоносное ПО сыпется как из рога изобилия, используя самые разные методы атаки – от незаметных и изощрённых до простых и прямолинейных, как лом. Но знание – сила. Вооружившись нужной информацией, Вы можете снизить опасность заболевания. Поэтому мы предлагаем небольшой обучающий курс о вредоносном ПО, призванный рассказать вам о том, что оно собой представляет, каковы его симптомы, как происходит заражение, как выбрать лекарство и как противостоять вирусам в будущем.

Что такое вредоносное ПО?

Вредоносное программное обеспечение (или вредоносное ПО) – это собирательный термин, обозначающий вредоносную программу или код, который может причинить ущерб компьютерной системе.

Вредоносное ПО умышленно создается враждебным, назойливым и агрессивным. Оно стремится проникнуть в систему, нанести урон, частично перехватить контроль над некоторыми процессами или вовсе вывести из строя компьютеры, компьютерные системы, сети, планшетные и мобильные устройства. Как и человеческий вирус гриппа, оно мешает нормальной работе.

Цель вредоносного ПО – получение незаконной прибыли за Ваш счёт. Несмотря на то, что вредоносное ПО не может повредить аппаратное обеспечение системы или сетевое оборудование, оно может похитить, зашифровать или удалить Ваши данные, изменить функции

компьютера или перехватить контроль над ними. Кроме того, оно может без Вашего ведома следить за активностью компьютера.

Как понять, что система заражена вредоносным ПО?

Вредоносное ПО может проявлять себя множеством способов. Вот лишь некоторые наиболее распространённые признаки, которые указывают на наличие вредоносного ПО в Вашей системе:

- Компьютер начинает работать медленно. Одно из основных последствий проникновения вредоносного ПО в операционную систему – снижение скорости её работы независимо от того, просматриваете ли Вы веб-страницы или используете локальные приложения.
- На экране начинает периодически появляться навязчивая реклама. Неожиданные всплывающие рекламные сообщения являются типичным признаком заражения компьютера вредоносным ПО. Чаще всего они вызваны особой формой вредоносного ПО – рекламным ПО. Более того, всплывающие рекламные блоки обычно связаны с другими скрытыми угрозами со стороны вредоносного ПО. Поэтому важно помнить: если на экране внезапно появляется сообщение «ПОЗДРАВЛЯЕМ! ВЫ ВЫИГРАЛИ МИЛЛИОН РУБЛЕЙ!», не нажимайте на него! Какой бы приз не обещала реклама, заплатить всё равно придется Вам, причём заплатить много.
- Компьютер часто выдает сбои, «зависает» или отображает «синий экран смерти», который в системах Windows свидетельствует о наличии критической ошибки.
- Вы замечаете, что по непонятным причинам уменьшилось количество свободного места на диске. Возможно, винить в этом следует разросшееся вредоносное ПО, которое скрывается где-то на жёстком диске.
- Интернет-активность системы странным образом возросла.
- Интенсивность использования системных ресурсов чрезмерно высока, а охлаждающий вентилятор компьютера постоянно работает на полной скорости. Это верный признак того, что вредоносное ПО использует системные ресурсы в фоновом режиме.
- Начальная страница браузера изменена без Вашего разрешения. Нажатие на ту или иную ссылку переводит Вас на нежелательные веб-страницы. Обычно это свидетельствует о

том, что Вы нажали на то самое всплывающее сообщение с «поздравлениями», после чего на компьютер было установлено нежелательное программное обеспечение. В аналогичных случаях работа браузера может значительно замедлиться.

- В браузере внезапно появляются новые панели инструментов, расширения или плагины.
- Антивирусная программа перестаёт работать, Вам не удается её обновить, так что Вы остаетесь беззащитными перед лицом коварного вредоносного ПО, отключившего её.
- Бывают и очевидные атаки вирусов, которые даже не пытаются маскироваться. Такую тактику выбирают программы-вымогатели: они заявляют о себе, сообщают о том, что похитили Ваши данные, а затем требуют выкуп за возврат файлов. НИКОГДА не платите вымогателям! Просто пригласите программиста. В худшем случае он просто переустановит Вам систему.
- И даже если система как будто в порядке, это ещё не повод для самоуспокоения, поскольку отсутствие новостей – далеко не всегда хорошая новость. Опасное вредоносное ПО может спрятаться в недрах компьютера и делать свое грязное дело, не привлекая внимания: похищать пароли, файлы с конфиденциальными данными или использовать Ваш ПК для заражения других компьютеров.

Как атакует вредоносное ПО?

Атака вредоносного ПО может осуществляться множеством способов. Самые распространённые пути проникновения вредоносного ПО в систему – через Интернет и через электронную почту. То есть это может случиться в любое время, когда Вы работаете онлайн.

Вредоносное ПО может проникнуть на Ваш компьютер, когда Вы (сделайте глубокий вдох) просматриваете взломанные злоумышленниками веб-сайты, открываете демонстрационные версии игр, загружаете заражённые музыкальные файлы, устанавливаете новые панели инструментов незнакомого производителя, загружаете программы из непроверенных источников, открываете вложения вредоносных сообщений электронной почты. Словом, это может произойти в любой ситуации, когда Вы загружаете контент из всемирной паутины на устройство, на котором нет достаточно сильного антивируса.

Вредоносные объекты часто скрываются в обычных на первый взгляд программах – и вероятность этого возрастает в том случае, если Вы загружаете их не через надёжный магазин приложений, а с веб-сайтов или через сообщения. Во время установки приложений важно обращать внимание на предупреждающие сообщения, особенно если они запрашивают разрешение на доступ к Вашей электронной почте или другим персональным данным.

Наилучший способ уберечь себя от опасностей – устанавливать мобильные приложения только из проверенных источников, доверять только надёжным сторонним производителям приложений, а также всегда загружать программы непосредственно с веб-сайта производителя – и никогда с других веб-сайтов. Помните, что киберпространство полно злоумышленников и злодеев, готовых бросить Вам наживку – предложить «ускоритель Интернета», новый диспетчер загрузок, программы для очистки жесткого диска или альтернативный поисковой сервис.

Коварные планы вредоносного ПО не были бы столь успешны без самой важной составляющей – ***вас***. Они используют вашу доверчивость, вашу привычку открывать сообщения электронной почты и переходить к вложениям, которые только выглядят безобидными, они эксплуатируют ваше желание скорей нажать на ссылку и установить программу, источнику которой на самом деле нельзя доверять. Важно понимать, что мы ни в коем случае не хотим пристыдить вас, поскольку злоумышленники могут обхитрить даже самых опытных пользователей и заставить их установить вредоносное ПО.

Даже если вы устанавливаете программу из надёжного источника, вы можете не обратить внимание на то, что она запрашивает разрешение на установку еще одного приложения, которое вы не собирались устанавливать. Эта дополнительная программа часто замаскирована под важный компонент, которым она часто не является.

Применение еще одного метода, использующего ресурсы социальной инженерии, наблюдалось экспертами Malwarebytes в Великобритании. Злоумышленники атаковали пользователей за счёт функции прямого платежа, распространённой в мобильных устройствах. Посещая определённые веб-сайты, пользователи непреднамеренно нажимали на невидимые кнопки, после чего злоумышленники, зная телефонные номера жертв, выставляли им счета прямо через мобильную сеть и успешно списывали средства в свою пользу.

Будем честными: атака вредоносного ПО может быть настолько искусной, что её невозможно заметить. Велика вероятность, что даже простое посещение вредоносного веб-сайта и просмотр его страницы

и/или рекламного баннера приводят к теневой загрузке нежелательных объектов.

С другой стороны, если вы не используете надлежащую защитную программу, то заражение вредоносным ПО и его последствия остаются целиком на вашей совести.

Каковы наиболее распространённые формы вредоносного ПО?

Вот самые известные экспонаты в галерее вредоносного ПО:

- **Рекламное ПО** – это нежелательная программа, написанная для того, чтобы забрасывать экран компьютера рекламными сообщениями (чаще всего во время использования браузера). Как правило, подобные объекты используют мошеннические методы, чтобы принудить пользователя установить их на свой ПК, планшетный компьютер или мобильное устройство: они выдают себя за обычные программы или проникают в систему в качестве «дополнительной нагрузки» при установке других приложений.
- **Шпионские программы** – это вредоносное ПО, которое скрытно наблюдает за действиями пользователя компьютера и пересылает накопленные данные своим разработчикам.
- **Вирусы** – это вредоносное ПО, которое прикрепляется к другой программе и при её запуске (что обычно происходит по неосторожности пользователя) начинает самовоспроизводиться и модифицировать другие приложения на компьютере, внедряя в них элементы своего вредоносного кода.
- **Черви** – это тип вредоносного ПО, напоминающий вирусы. Они также обладают способностью к самокопированию, проникают на компьютер через сеть и обычно наносят вред, удаляя данные или файлы.
- **Троянские программы**, также обозначаемые как вредоносные программы типа «троянский конь», – это один из самых опасных типов вредоносного ПО. Они обычно стремятся обмануть вас, маскируясь под полезные программы. После того как троянская программа проникла в систему, злоумышленники получают несанкционированный доступ к зараженному компьютеру. Троянские программы используются для похищения финансовой информации, а также для того, чтобы проторить дорогу другим вредоносным объектам, например вирусам и программам-вымогателям.

- **Программы-вымогатели** – это вредоносное ПО, которое блокирует Ваше устройство и/или шифрует Ваши файлы, а затем заставляет Вас заплатить выкуп за их возврат. Программы-вымогатели считаются излюбленным оружием киберпреступников, поскольку они дают им возможность быстро получить значительную прибыль в криптовалюте, операции с которой сложно отследить. Код, на котором основываются программы-вымогатели, можно без проблем получить на чёрном интернет-рынке, а защититься от него всегда непросто.

- **Руткиты** – это вредоносное ПО, которое предоставляет злоумышленникам права администратора на заражённом компьютере. Обычно они остаются незамеченными для пользователя, других программ и самой операционной системы.

- **Клавиатурные шпионы** – это вредоносное ПО, которое записывает, на какие клавиши нажимают пользователи, сохраняет накопленную информацию и отправляет её своим авторам, которые извлекают из полученных данных важные сведения, например имена пользователей, пароли или реквизиты кредитных карт.

- **Программы для теневого вредоносного майнинга**, также иногда обозначаемые как программы для «криптоджекинга», – это тип вредоносного ПО, который получает все более широкое распространение. Эти объекты используются для скрытого майнинга криптовалют и обычно устанавливаются с помощью троянской программы. В результате посторонние лица могут использовать ресурсы Вашего компьютера, чтобы добывать криптовалюты, например, биткойн или монеро. Не давая Вам зарабатывать деньги на мощности своего компьютера, криптомайнеры отправляют полученные «монеты» на собственные счета. Программы для вредоносного майнинга фактически крадут ресурсы чужих систем с целью получения прибыли.

- **Эксплойты** – это вредоносное ПО, которое использует ошибки и уязвимости в системе, чтобы передать своим авторам контроль над ней. Как и другие угрозы, эксплойты нередко распространяются через вредоносную рекламу: она может отображаться даже на обычных веб-сайтах, которые извлекают вредоносный контент из скомпрометированных веб-сайтов. В случае успешной атаки эксплойт пытается проникнуть в систему посредством теневой загрузки. Пользователю даже не приходится нажимать на кнопку. Достаточно просто посетить вполне благонадёжный веб-сайт в неудачный день.

Поражает ли вредоносное ПО компьютеры Mac?

Бытует мнение, что устройства Mac и iPad невосприимчивы к вирусам (и поэтому не нуждаются в антивирусных программах). В целом, это правда. По крайней мере, в прошлом наблюдались длительные периоды затишья.

Системы Mac имеют те же уязвимости (и связанные с ними симптомы заражения), что и компьютеры под управлением Windows, так что их надёжность в этом отношении не абсолютна. Так, встроенная защита Mac от вредоносного ПО не может заблокировать все рекламное ПО и все шпионские программы, которые проникают на компьютер вместе с загружаемыми мошенническими программами. Троянские программы и клавиатурные шпионы также представляют угрозу. Программа-вымогатель, написанная специально для системы Mac, была обнаружена в марте 2016 года, когда атака на основе троянской программы затронула более 7000 компьютеров Mac.

Поражает ли вредоносное ПО мобильные устройства?

Киберпреступники и производители вредоносного ПО отлично себя чувствуют на рынке мобильных устройств. Ведь смартфоны в действительности являются портативными компьютерами со множеством функций. Кроме того, они представляют собой сокровищницу персональных данных, финансовой информации и других ценных сведений, которые привлекают желающих заработать деньги нечестным путем.

К сожалению, почти экспоненциальный рост количества смартфонов повлек за собой всплеск активности вредоносных программ, пытающихся воспользоваться уязвимостями этих устройств. Рекламное ПО, троянские программы, шпионские программы, черви и программы-вымогатели – все эти вредоносные объекты могут проникнуть на Ваш телефон самыми различными способами. Переход по рискованной ссылке или загрузка непроверенного приложения – лишь самые очевидные источники проблем. Однако Вы также можете заразить телефон через электронную почту, тексты или даже через подключение Bluetooth. Кроме того, некоторые типы вредоносного ПО, например черви, распространяются непосредственно с одного телефона на другой.

Кроме того, атаковать пользователей мобильных устройств может быть намного проще. В большинстве случаев они не защищают свои телефоны так же надёжно, как и компьютеры, не устанавливают защитные программы или вовремя не обновляют операционную систему. Это делает их уязвимыми даже для примитивного

вредоносного ПО. Экраны мобильных устройств невелики, и пользователь просто не в состоянии уследить за всем, что происходит в системе. Подозрительная активность, которая в условиях ПК обычно свидетельствует об атаке вируса, может остаться незамеченной, как в случае со шпионскими программами.

Заражённые мобильные устройства еще опасней заражённых ПК. Взломав смартфон, злодеи могут следить за каждым Вашим шагом с помощью камеры, подслушивать Ваши разговоры. Что ещё хуже, вредоносное ПО, нацеленное на мобильный банкинг, перехватывает входящие звонки и текстовые сообщения, чтобы обойти двухступенчатую авторизацию, используемую многими банковскими приложениями.

В среде вредоносного ПО для мобильных устройств наиболее распространены объекты, поражающие две основные операционные системы – Android от Google и iOS от Apple. Android лидирует на рынке – с этой операционной системой продается 80 процентов всех смартфонов; доля iOS составляет 15 процентов. Поэтому нет ничего удивительного в том, что более популярная платформа Android привлекает намного больше вредоносного ПО, чем iPhone. Давайте рассмотрим каждую из них в отдельности.

Как понять, что устройство Android заражено вредоносным ПО?

К счастью, есть несколько признаков, по которым можно безошибочно определить, что устройство Android подверглось заражению. Итак, Вы были атакованы, если замечаете следующее:

- Внезапное появление всплывающих окон с навязчивой рекламой. Если они появляются из ниоткуда и направляют Вас на схематично оформленные веб-сайты, то Вы, вероятно, установили приложение, в котором скрыто рекламное ПО. Поэтому не нажимайте на рекламный блок.
- Странный всплеск использования данных. Вредоносное ПО может расходовать значительные части Вашего тарифного плана, чтобы отображать рекламу и отправлять злоумышленникам похищенную на телефоне информацию.
- Подозрительные суммы в выставленных к оплате счетах. Такое случается, когда вредоносное ПО совершает звонки и отправляет текстовые сообщения на платные номера.

- Быстро исчезающий заряд аккумулятора. Вредоносное ПО потребляет ресурсы телефона и, соответственно, быстрее разряжает аккумулятор.
- Абоненты из Вашего списка контактов сообщают о странных звонках и текстовых сообщениях, поступающих с Вашего телефона. Вредоносное ПО самовоспроизводится, отправляя свои копии с одного устройства на другое по электронной почте, и даже в текстовых сообщениях, предлагающих другим пользователям перейти по специальной ссылке.
- Перегрев телефона при одновременном снижении его производительности. Существует, например, троянская программа, которая проникает в систему Android и приносит за собой крайне агрессивный установщик; он в свою очередь перегружает процессор, вызывает чрезмерный нагрев телефона и истощает аккумулятор (иногда даже вызывая его деформацию), что, разумеется, приводит устройство Android в полную негодность.
- Неожиданные приложения на экране. Иногда вредоносные программы скрытно проникают в систему в качестве «дополнительной нагрузки» при установке других приложений. Это происходит из-за того, что Android позволяет переходить напрямую из Google Play в другой магазин, например Amazon, который мог упустить тот или иной вредоносный объект.
- Телефон сам включает Wi-Fi и мобильный Интернет. Это еще один способ распространения вредоносного ПО, когда оно игнорирует Ваши настройки и открывает каналы для заражения.

Ниже мы расскажем Вам о том, что следует предпринять, если на Ваше устройство Android все-таки проник вирус. Как понять, что iPhone или iPad заражены вредоносным ПО?

Очень примечательная история произошла в 2016 году, когда на iPhone представителя известной организации по защите прав человека, расположенной в Объединенные Арабских Эмиратах (ОАЭ), пришло текстовое SMS-сообщение с обещанием раскрыть «новые секреты» о пытках заключенных в тюрьмах ОАЭ. Получателю предлагалось перейти по прилагаемой ссылке. Он не стал этого делать, а отправил сообщение специалистам в области кибербезопасности, которые изучили текст и обнаружили эксплойт, способный превратить телефон жертвы в настоящего цифрового шпиона.

Второй случай предполагает, что пользователь сам делает iPhone уязвимым за счёт взлома (джейлбрейка), который снимает ограничения, наложенные компанией Apple на использование телефона, – в первую очередь это касается запрета на установку приложений не из магазина App Store. Компания Apple тщательно проверяет представленных в нём разработчиков и накладывает на них санкции даже в том случае, если вредоносному ПО удается пробраться в систему вслед за обычным приложением.

И ещё. Несмотря на то что открытая атака вредоносного ПО маловероятна, использование iPhone не защитит Вас от мошеннических звонков и текстовых сообщений. Если Вы нажмёте на ссылку в сообщении, полученном от неизвестного отправителя (или от пользователя, который выдает себя за другого), то Вы можете попасть на мошеннический сайт, где Вам предложат ввести свой пароль или другие личные данные. Так что не нужно недооценивать изобретательность киберпреступников. Всегда действуйте осторожно.

Кого атакует вредоносное ПО?

Ответ прост: кого угодно. В мире миллиарды устройств, принадлежащих частным пользователям. С их помощью люди совершают банковские операции, покупки в розничных магазинах, а также передают и сохраняют самую разную информацию, которую кое-кто не прочь похитить. Для злоумышленников мобильные устройства – лишь среда распространения рекламного ПО, шпионских программ, клавиатурных шпионов и вредоносной рекламы. Поэтому они стремятся создавать новые виды вредоносных объектов и доставлять как можно больше их копий на различные устройства, прилагая для этого по возможности минимум усилий.

Криптомайнеры и распространители программ-вымогателей одинаково опасны для своих целей. Их жертвами становятся не только частные лица, но и целые предприятия, больницы, муниципальные учреждения и магазины розничной торговли.

Потребители являются не единственной целью злоумышленников, создающих шпионские программы. Если вы используете свой смартфон или планшетный компьютер на рабочем месте, хакеры могут атаковать организацию вашего работодателя за счет уязвимостей, заложенных в системе мобильных устройств. Более того, группам реагирования на инциденты в области компьютерной безопасности может быть не под силу выявлять атаки, которые совершаются через мобильные устройства во время использования корпоративной электронной почты.

Как удалить вредоносное ПО?

Если Вы подозреваете, что на Вашем устройстве завелось вредоносное ПО, или просто хотите перестраховаться, пожалуйста, выполните несколько простых шагов.

Самой популярной и эффективной программой по защите компьютеров и мобильных телефонов на сегодняшний день считается «Мэлвэрбайтс» (**Malwarebytes**). Существуют разные виды программ – для Windows, для Мака и для Андроида. Установите программу и запустите проверку. Указанные программы выполняют поиск и устраняют все вредоносные объекты, обнаруженные на вашем устройстве.

После того как система очищена от вирусов, рекомендуется сменить пароли – не только в учетной записи компьютера или мобильного устройства, но и в электронной почте, социальных сетях, часто посещаемых онлайн-магазинах, а также в банковских и биллинговых сервисах.

Как защититься от вредоносного ПО?

Оставайтесь бдительны. Обращайте особое внимание на домены, которые представляют собой странную комбинацию букв и отличаются от привычных com, org, edu, biz и других, поскольку это может указывать на веб-сайт в группе риска.

На всех устройствах следите за возможным появлением ранних признаков заражения вредоносным ПО, чтобы не дать ему закрепиться в недрах системы.

Во время работы в сети Интернет не нажимайте на рекламные блоки во всплывающих окнах. Не открывайте вложения в электронных письмах, которые пришли от незнакомого отправителя, не загружайте программы с непроверенных веб-сайтов или через пиринговые сети.

Всегда поддерживайте операционную систему, браузеры и плагины в актуальном состоянии, поскольку своевременное получение обновлений поможет не подпускать киберпреступников слишком близко.

Пользователям мобильных устройств рекомендуется устанавливать приложения только из магазина Google Play (для пользователей iPhone единственным магазином является App Store). Всякий раз перед загрузкой нового приложения проверяйте его рейтинги и прилагаемые отзывы. Если рейтинги невысоки, а количество загрузок невелико, то такое приложение лучше не устанавливать.

Не загружайте приложения из сторонних источников. Мы рекомендуем вовсе отключить эту функцию в меню устройства Android. Для этого выберите пункт «Настройки» и перейдите к разделу «Безопасность». Затем отключите параметр «Неизвестные источники» – в этом случае Вы будете загружать приложения только из магазина Google Play (в современных версиях Андроида настройки могут отличаться).

Не нажимайте на странные непроверенные ссылки в электронных письмах, текстах и сообщениях **WhatsApp**, отправленных неизвестным отправителем. Следует также избегать странных ссылок, полученных от друзей или пользователей в списке контактов, – за исключением случаев, когда Вы убедились в их безопасности.

Стремясь защитить свой бизнес и избавить компьютерные сети от вредоносных приложений, организации могут применять строгие правила безопасного использования мобильных устройств, а также устанавливать средства защиты мобильных устройств для реализации этих правил. Это жизненно необходимо для современной корпоративной среды, в которой множество операционных систем совместно работают в различных зданиях.

Наконец, обзаведитесь надежной антивирусной программой. Она должна обладать многоуровневой защитой, позволяющей проверять систему и обнаруживать вредоносное ПО, например рекламное ПО и шпионские программы, а также в реальном времени проактивно блокировать другие угрозы, например атаки программ-вымогателей. Антивирусная программа также должна быть способна устранять последствия атак, восстанавливать ущерб, нанесённый вредоносным ПО, и возвращать системе нормальную функциональность.

Адрес для скачивания программы «Мэлвэрбайтс» - ru.malwarebytes.com. Одновременно рекомендуется ставить и бесплатную версию антивирусной программы типа **Avast**, **AVG** или **Kaspersky** и для проверки запускать обе программы одну за другой – так будет надёжнее.

ПРАКТИЧЕСКИЙ СОВЕТ

Если вы установили на компьютере антивирусную программу, то это не означает, что она будет работать в автоматическом режиме без вашего участия. Антивирусную программу надо запускать вручную минимум раз в неделю и удалять вирусы и другое вредоносное ПО вручную. То же самое касается программы чистки компьютера **CCleaner**. Очень рекомендуем установить эту программу и регулярно

чистить свой диск от устаревших и ненужных файлов, которые тормозят работу компьютера. Можно также установить аналогичную программу под названием **Reg Organiser**. Выбор за вами.