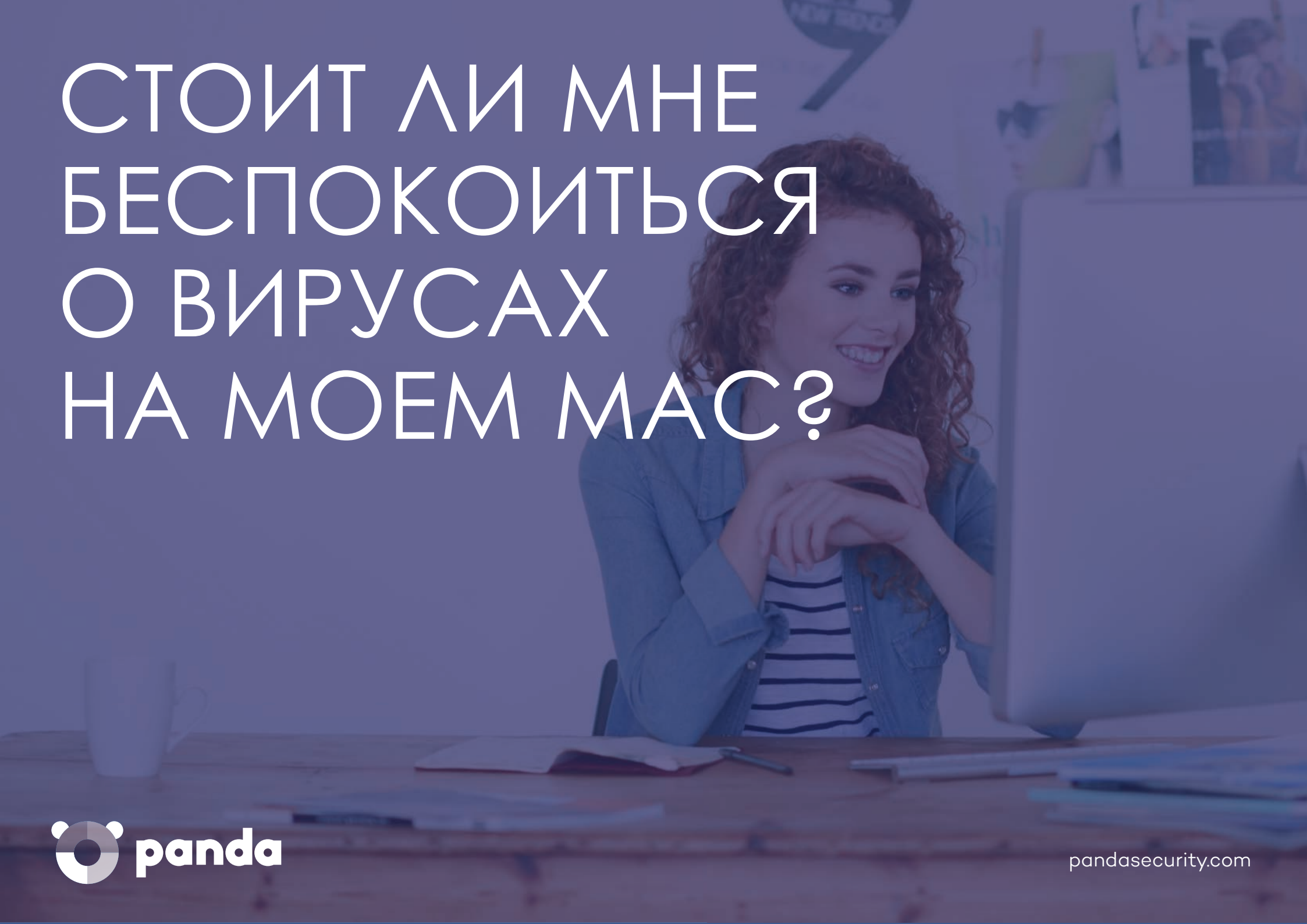
СТОИТ ЛИ МНЕ БЕСПОКОИТЬСЯ О ВИРУСАХ НА МОЕМ MAC?



panda

pandasecurity.com

01 Существуют ли проблемы безопасности в Mac OS X?

02 Это правда, что нет вирусов под Mac?

03 Что делает Apple для защиты своих пользователей?

04 Что можно сделать, чтобы минимизировать риск заражения?

“Mac OS X – это безопасная платформа, потому что вирусы Windows не влияют на нее"

Существуют ли в Mac OS X проблемы безопасности?

Форумы по IT-безопасности часто полны успокоительных комментариев для пользователей Apple, и все же: стоит ли Вам беспокоиться о безопасности Вашей системы Mac OS X? Стоит! Если рассматривать некоторые события, произошедшие после 2011 года, то Вы бы пришли к точно такому же выводу и без "экспертного" мнения тех, кто, к счастью, не пострадал от своих советов.

Любые обсуждения концепции безопасности систем Apple не являются однозначными. Причем это не связано с предсказуемой озабоченностью производителя защитить свои продукты от внешних угроз: такая неоднозначность возникает в силу «особой практики» использования продукции данного бренда. Правда заключается еще в том, что Apple в свое время остался в стороне от многих инцидентов безопасности, и это было связано, в основном, с его небольшими продажами по сравнению с основным конкурентом Windows.

Действительно, было бы странно полагать, что хакеры стали бы массово разрабатывать вредоносные программы под такую нишевую платформу, и еще более странно было бы то, что Apple внедрял бы необходимые меры по предотвращению взлома своих пользователей, если в прошлом таких потребностей не возникало.

Apple в 2012 году имел долю мирового рынка настольных компьютеров всего 6%. Создавать вредоносные программы под Mac не было выгодным мероприятием, а производителю, в свою очередь, также не совсем выгодно было внедрять и развивать средства защиты от того, что практически не существовало.

Ранее на сайте Apple был вполне однозначный совет относительно безопасности.

Нельзя заразиться вирусами для ПК

"Mac не подвержен тысячам вирусов, преследующих компьютеры на базе Windows. Это благодаря встроенной системе защиты в Mac OS X, которая обеспечивает Вашу безопасность без каких-либо усилий с Вашей стороны".

Защитите Ваши данные. Ничего не делая

"Практически без усилий с Вашей стороны OS X защищает Вас от вирусов и других вредоносных приложений или программ. Например, срывает атаки хакеров через так называемую технику «песочница». Она ограничивает действия, которые могут выполнять программы на Вашем Mac, и файлы, к которым они могут получить доступ, а также определяет список других программ, которые они могут запускать".

Они описывают вирусы для ПК как единственную потенциальную проблему и говорят о защите, встроенной в операционную систему Apple, как средстве, обеспечивающем безопасность платформы. По их мнению, платформа настолько безопасна, что пользователям не следует предпринимать каких-либо дополнительных усилий для своей защиты.

Таким образом, проблемы (якобы!) не существует.

Тем не менее, в июне 2012 года тон сообщения несколько поменялся.

Создан, чтобы быть безопасным

"Встроенные в OS X средства защиты обеспечивают Вашу безопасность от неосознанной загрузки вредоносных программ на Ваш Mac".

Безопасность. Встроена

"OS X разработана с использованием мощных и передовых технологий, которые упорно трудятся над обеспечением безопасности Вашего Mac. Например, срывает атаки хакеров через так называемую технику «песочница». Она ограничивает действия, которые могут выполнять программы на Вашем Mac, и файлы, к которым они могут получить доступ, а также определяет список других программ, которые они могут запускать".

Здесь уже нет упоминания о вирусах для ПК – легко понять, почему. Уже не было возможности игнорировать существование специальных вирусов под Mac.

Кроме того, они отозвали свое предложение пользователям ничего не делать для защиты своих систем.

В июне 2012 года Apple впервые заговорила о вредоносных программах в своей программной речи на Всемирной конференции разработчиков (WWDC) в рамках презентации своей технологии Gatekeeper, которая «могла бы помочь бесплатно защитить систему от вредоносных программ».

Все это доказывает, что Apple всегда были уязвимы для вредоносных программ, также как и системы его конкурентов.

Окончательно это было продемонстрировано в конце 2011 года, когда провайдер решений безопасности Apple компания Intego обнаружила троян, который они окрестили как «Flashback».

Данная вредоносная программа использовала уязвимости в Java, которые были известны в течение нескольких недель, чтобы заразить свыше 600 000 пользователей Mac в течение нескольких месяцев. Кроме того, 274 из них были расположены в Купертино, штат Калифорния, - это штаб-квартира компании Apple.

Любой продвинутый пользователь Windows знает, что многие инфекции весьма заметны и часто приводят к изменениям в системе, которые могут указывать на наличие вредоносных программ на Вашем ПК.

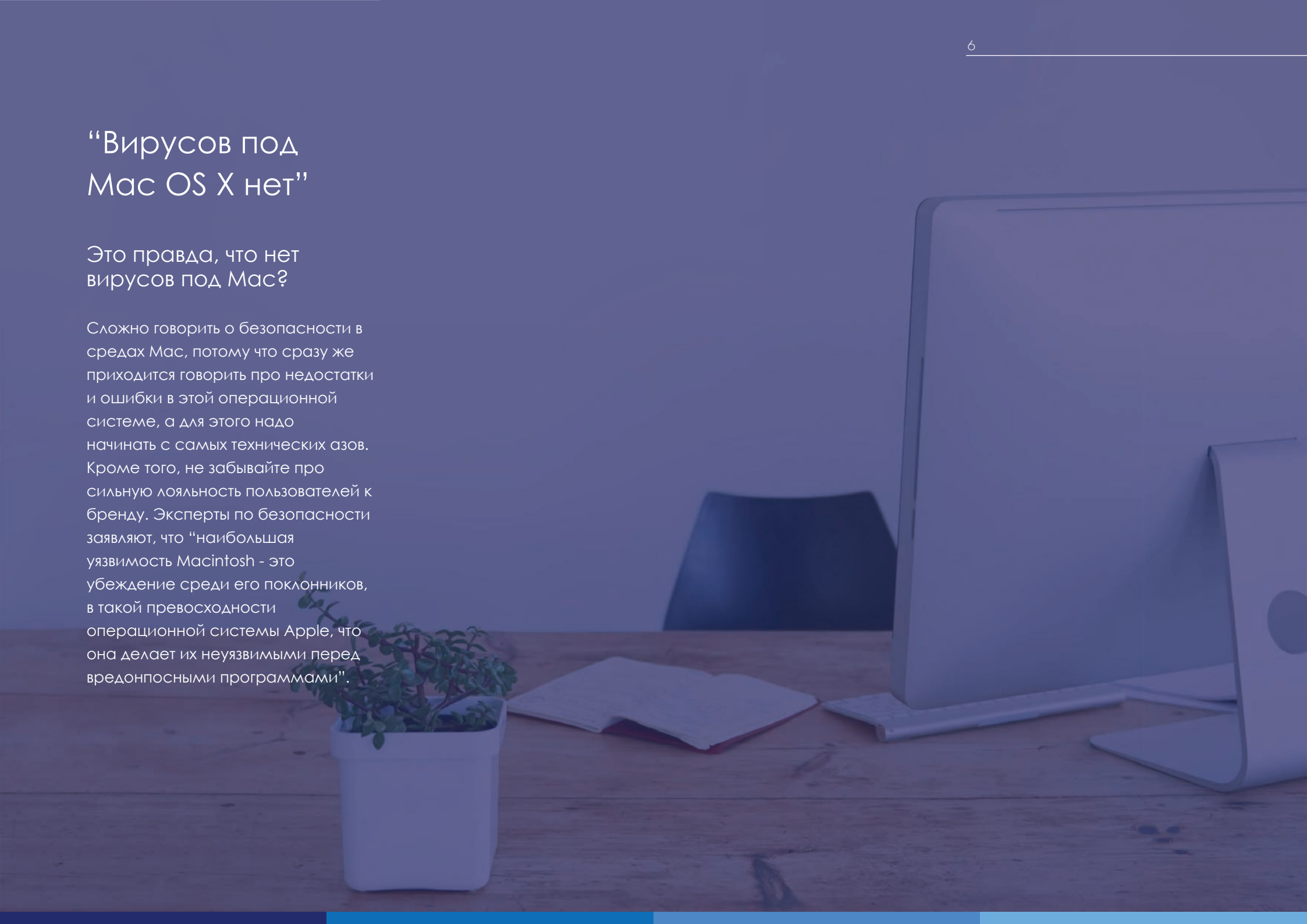
Однако Ваша платформа Mac может быть заражена в течение длительного времени, а Вы можете об этом и не подозревать, потому что Mac OS X дарит своим пользователям ложное чувство безопасности, что в конечном итоге крайне вредно для безопасности Ваших данных.

Платформы Apple всегда были уязвимы для вредоносных программ, также как и системы его конкурентов.

“Вирусов под Mac OS X нет”

Это правда, что нет вирусов под Mac?

Сложно говорить о безопасности в средах Mac, потому что сразу же приходится говорить про недостатки и ошибки в этой операционной системе, а для этого надо начинать с самых технических азов. Кроме того, не забывайте про сильную лояльность пользователей к бренду. Эксперты по безопасности заявляют, что “наибольшая уязвимость Macintosh - это убеждение среди его поклонников, в такой превосходности операционной системы Apple, что она делает их неуязвимыми перед вредонпосными программами”.



Строго говоря, вирус представляет собой вредоносную программу, встроенную в другую программу или файл, который может распространяться на другие компьютеры.

Тем не менее, Flashback не был вирусом, а был трояном, который после установки скачивал программное обеспечение, специально предназначенное для кражи банковских данных, паролей браузера и другой конфиденциальной информации с компьютера пользователя. Дело в том, что мы должны говорить о вредоносных программах и безопасности в целом, а не только о вирусах.

Крайне опасно говорить, что в мире не существует вирусов, которые негативно влияют на системы Mac: это приводит к заблуждениям, а с точки зрения безопасности заблуждения, в конечном итоге, приводят к финансовым потерям.

Помимо Flashback существуют и другие вредоносные программы под Mac, которые негативно влияли на его пользователей:

Pintsized

Вредоносная программа, которая использует уязвимости в Java, чтобы создать дыру безопасности в компьютере и позволить хакеру получить удаленный контроль над системой.

CoinThief

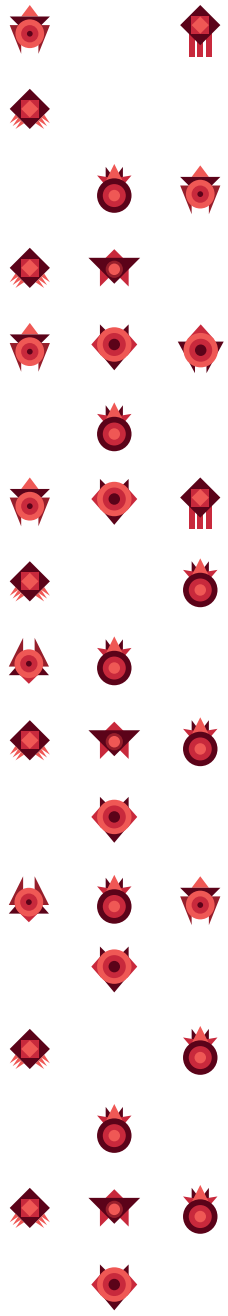
Вредоносная программа, которая пытается представить себя в качестве вполне легитимного приложения для осуществления платежей в Интернете, но которая вполне реально крадет цифровые деньги Bitcoin.

Icefog

Вредоносная программа под различные платформы, использованная для кибер-шпионажа в Японии, Южной Корее и других частях Азии.

Mac Defender

Ложный антивирус, который вынуждает пользователей регистрировать программу и платить якобы за «защиту».



Эффект от вредоносных программ всегда одинаков независимо от того, являются ли они вирусами, трояна-ми, руткитами или программами-вымогателями (ransomware)… Тут нет необходимости точно знать весь этот технический жаргон. Все, что Вам необходимо знать, - это то, что существуют вредоносные программы, которые МОГУТ повлиять на Вашу систему Mac OS X, а Ваши финансы окажутся в опасности.

Крайне опасно говорить, что в мире не существует вирусов, которые негативно влияют на системы Mac: самая серьезная уязвимость Mac – это слепая вера поклонников Apple в то, что их операционная система является самой лучшей и надежно защищает их от вредоносных программ.

“Вам не стоит волноваться о безопасности Mac”

Что делает Apple для защиты своих пользователей?

Даже если некоторые пользователи отрицают это, всего равно следует сказать, что идет война, в ходе которой, безусловно, способы атаки и защиты постоянно развиваются. Существует сообщество людей, чья финансовая мотивация по разработке вредоносных программ возрастает параллельно тому, как растут продажи Mac OS X. Следовательно, компания Apple разрабатывает защиту и защищает своих пользователей… или так может показаться.

Основная проблема заключается в том, что Apple слишком поздно вышел на сцену, где теперь Microsoft сильно закален в боях после череды серьезных поражений несколько лет назад. Приход Интернета показал начало экспоненциального роста количества вредоносных программ, а Windows 95, 2000 и XP были теми платформами, с которыми Microsoft пытался практически самостоятельно справиться с ситуацией. До этого подобных случаев не было, и компании пришлось моментально реагировать на них под сильным давлением миллионов зараженных систем.

В результате такой крутой ситуации Microsoft стал компанией, твердо приверженной принципам безопасности с четким планом выхода обновлений безопасности и способностью оперативно реагировать на ситуацию, выпуская патчи и обновления для своих операционных систем.

В случае же с Apple все как раз наоборот. Он выпускает свои обновления только тогда, когда сочтет это необходимым, и в случае с Flashback компании **потребовалось шесть недель на выпуск патчей, исправляющих эту уязвимость**, в то время как эти патчи уже были разработаны и выпущены компанией Oracle.

Были и другие подобные случаи, например, с Icefog, когда **Apple потребовалось две недели**, чтобы добавить сигнатурный файл в свой антивирус Xprotect. А в это время Icefog продолжал заражать компьютеры пользователей, которые даже и не подозревали о наличии проблемы. **Сравните это с провайдерами облачных решений безопасности, которые предоставляют обновления в считанные минуты!**

Apple также не имеет и четкой политики, если речь заходит об анонсах окончания поддержки своих продуктов: например, взять случаи с версиями 10.9 и 10.9.1, когда некоторые добавленные патчи не были доступны для более ранних версий (Lion и Mountain Lion). И только с выходом версии 10.9.2 компания опубликовала исправления в системе безопасности для защиты пользователей Lion и Mountain Lion от вредоносных программ. Но в этом случае были упущения с версией Snow Leopard (10.6).

Поэтому если у Вашей системы версия 10.6, то срочно обновляйте ее!

Как результат, **пользователи не знают, когда выходят решения и вышли ли они уже, если у них не последняя версия операционной системы**. Приверженность Apple к безопасности просто не соответствует этой задаче. Держать пользователей «в темноте» - это основная стратегия компании и, возможно, причина этого заключается в том, что компании слишком тяжело расстаться с имиджем «неуязвимой платформы», который был очень выгоден ей в прошлом.

Apple стала постоянно включать существенные изменения в свои операционные системы для повышения уровня безопасности.

С другой стороны, начиная с 2009 года, компания Apple стала постоянно включать существенные изменения в свои операционные системы для поддержки уровня безопасности. Вот сводка таких изменений:

- **Leopard (10.5)**
  «Песочница», карантин файлов и файервол приложений.
- **Snow Leopard (10.6)**
  Антивирус Xprotect.
- **Mountain Lion (10.7)**
  Gatekeeper.

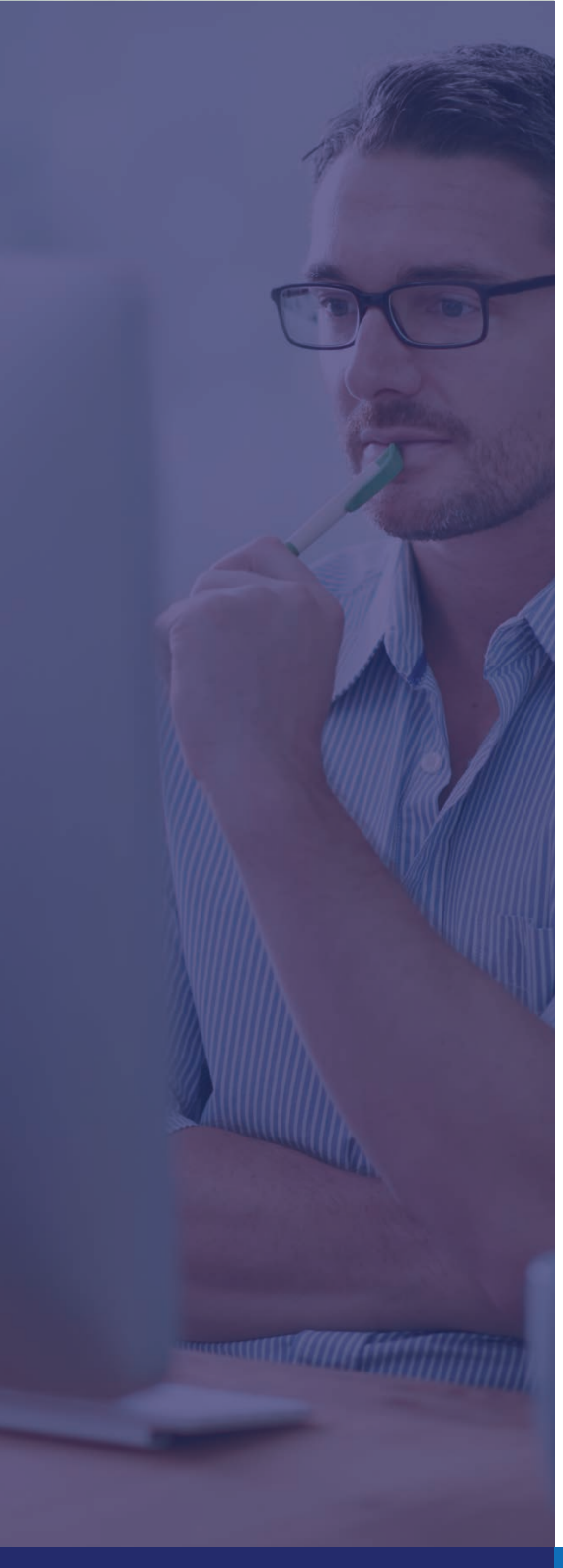
Начинают появляться «антитела» Mac OS X, как будто это биологический организм, и хотя это серьезное нововведение связано с безопасностью операционной системы, оно имеет такой же эффект, как и Security Essentials в Windows: т.к. предоставление безопасности со стороны Apple является частью базовой установки операционной системы, то создатели вредоносных программ уже знают о ее наличии, поэтому они концентрируют свои усилия на развитие контрмер для борьбы с защитой.

Вот почему пользователям необходимо дополнять основной уровень безопасности Apple хорошим сторонним антивирусом.

Вот почему пользователям необходимо дополнять основной уровень безопасности Apple хорошим сторонним антивирусом.

Что можно сделать, чтобы минимизировать риск заражения?

Здравый смысл и разумный подход являются ключевыми моментами, позволяющими избежать нежелательных заражений. Зная, что Ваша система уязвима, будьте осторожны при работе с информацией, доступной на Ваших устройствах, установите хороший антивирус и поддерживайте его в обновленном состоянии, а также избегайте подозрительных файлов и веб-сайтов - вот первые шаги по защите Вашего компьютера от кибер-атак.



Возвращаясь к 2011 году, Apple гордо заявил на своем сайте, что его система обладает устойчивым иммунитетом к вирусам для ПК. И на тот момент в той или иной степени такое заявление было правдивым: в основной своей массе, вирусы, написанные для Windows, действительно не работали на Mac OS X.

С появлением специальных вредоносных программ под Mac OS X, угрозы для Windows все еще оставались потенциальным источником проблем для гетерогенных окружений и даже негативно влияли на корпоративный имидж: представьте себе, что Вы отправляете своему клиенту предложение с вложением, зараженным вирусом для ПК. Кстати, сторонняя статистика показывает, что 43% вредоносных программ под Mac OS X являются «родственниками» вредоносных программ под Windows.

Защищаете ли Вы свои собственные системы, ПК с Windows вокруг Вас или Ваш корпоративный имидж, Вы можете обеспечить своей системе Mac OS X достойный уровень безопасности благодаря нескольким простым мерам.

1. Ваш Mac уязвим

Имейте в виду следующую недвусмысленную истину: Ваша система Mac НЕ является неуязвимой. Ваш компьютер может быть заражен, а Ваша система, вместо того чтобы помочь Вам обнаружить вирус, может работать против Вас, т.к. Вы будете заблуждаться в том, что вирусы просто «не работают» на Mac.

2. Нужен хороший антивирус

Вне зависимости от версии Вашего Mac OS Вы получите существенные преимущества (с точки зрения безопасности), если будете использовать антивирус для Mac. Угрозы, находящиеся в обращении на текущий момент, направлены на преодоление встроенной защиты Apple. Чем больше антивирусов на рынке, тем больше усилий придется затрачивать хакерам на их преодоление: у вирусов будет значительно меньше шансов, если не будет монополии в вопросах безопасности.

3. Устанавливайте все обновления

Устанавливайте все обновления по мере того, как они появляются для Вашей версии операционной системы, а также для других приложений, установленных на Вашем компьютере.

4. Смотрите, какие файлы Вы запускаете

Facebook, Twitter и другие подобные сайты представляют собой типичный источник распространения угроз от так называемых «друзей». То же самое касается и вложений в электронных письмах от неизвестных отправителей и файлов, скаченных через P2P программы. Скачивайте и запускайте файлы только из надежных источников.

5. Отключите проблемное ПО

Java и Flash – это технологии с длинной историей ошибок и уязвимостей. Перейдите на панель безопасности Вашего браузера Safari и отключите модуль Java или нажмите «Manage website settings» («Управлять настройками веб-сайтов») в зависимости от версии браузера.

Надо усилить базовую безопасность Apple хорошим антивирусом.


panda