Проприетарное программное обеспечение часто является вредоносным

Оглавление Последние добавления

Проприетарное программное обеспечение, также называемое несвободным программным обеспечением, означает программное обеспечение, которое не уважает свободу и сообщество пользователей . Проприетарная программа ставит своего разработчика или владельца в положение власти над своими пользователями. Эта власть сама по себе является несправедливостью.

Цель этого справочника — показать на примерах, что изначальная несправедливость проприетарного программного обеспечения часто приводит к дальнейшей несправедливости: вредоносным функциям.

Власть развращает; разработчик проприетарной программы испытывает искушение спроектировать программу так, чтобы она плохо обращалась с пользователями. (Программное обеспечение, разработанное для функционирования таким образом, чтобы плохо обращаться с пользователем, называется вредоносным ПО .) Конечно, разработчик обычно делает это не из злого умысла, а скорее для того, чтобы получить больше прибыли за счет пользователей. Это не делает его менее отвратительным или более законным.

Поддаваться этому искушению стало все более частым явлением; в настоящее время это стандартная практика. Современное проприетарное программное обеспечение, как правило, является возможностью быть обманутым, навредить, запугать или обмануть.

Онлайн-сервисы не являются выпущенным программным обеспечением, но в отношении всех плохих аспектов использование сервиса эквивалентно использованию копии выпущенного программного обеспечения. В частности, сервис может быть разработан для плохого обращения с пользователем, и многие сервисы так и делают. Однако мы не перечисляем здесь примеры вредоносных плохих услуг по двум причинам. Во-первых, сервис (независимо от того, вредоносный он или нет) не является программой, копию которой можно установить, и у пользователей нет никакой возможности изменить ее. Во-вторых, настолько очевидно, что сервис может плохо обращаться с пользователями, если его владелец того пожелает, что нам вряд ли нужно это доказывать.

Однако большинство онлайн-сервисов требуют, чтобы пользователь запускал несвободное приложение. Приложение — это выпущенное программное обеспечение, поэтому мы перечисляем вредоносные функции этих приложений. Ненадлежащее обращение со стороны самого сервиса навязывается использованием приложения, поэтому иногда мы упоминаем и эти ненадлежащие обращения, но мы стараемся четко указать, что делает приложение, а что — ненадлежащая услуга.

Когда веб-сайт предоставляет доступ к сервису, он, скорее всего, отправляет несвободное программное обеспечение JavaScript для выполнения в браузере пользователя. Такой код JavaScript является выпущенным программным обеспечением, и он морально эквивалентен другим несвободным приложениям. Если он делает вредоносные вещи, мы хотим упомянуть об этом здесь.

Говоря о мобильных телефонах, мы упоминаем еще одну вредоносную функцию — отслеживание местоположения, которое вызывается базовой радиосистемой, а не конкретным программным обеспечением в них.

По состоянию на март 2025 года на страницах этого каталога перечислено около 650 примеров вредоносных функций (с более чем 750 ссылками, подтверждающими их), но наверняка есть еще тысячи, о которых мы не знаем.

В идеале мы бы перечислили каждый случай. Если вы столкнетесь с случаем, которого у нас нет, напишите нам на webmasters@gnu.org, чтобы рассказать нам о нем. Пожалуйста, включите ссылку на авторитетную статью, которая четко описывает вредоносное поведение; мы не будем перечислять элемент без документации, на которую можно сослаться.

Если вы хотите получать уведомления о добавлении новых элементов или внесении других изменений, подпишитесь на рассылку <www-malware-commits@gnu.org> .

Несправедливость или методы	**Продукты или компании**
Зависимости Задние двери (1) Цензура Принуждение Сокрытия Обман ДРМ (2) Мошенничество Несовместимость Неуверенность Вмешательство Тюрьмы (3) Манипуляция Устаревание Саботаж Подписки Наблюдение Привязи (4) Тираны (5) В трубе	Бытовая техника Автомобили Конференц-связь EdTech Игры Мобильные телефоны Веб-страницы Adobe Амазонка Яблоко Google Майкрософт

1. *Бэкдор:* любая функция программы, которая позволяет кому-либо, кто не должен контролировать компьютер, на котором она установлена, отправлять ей команды.
2. *Управление цифровыми ограничениями, или «DRM»:* функции, предназначенные для ограничения действий пользователей с данными на своих компьютерах.
3. *Тюрьма:* система, которая устанавливает цензуру на прикладные программы.
4. *Tether:* функциональность, требующая постоянного (или очень частого) подключения к серверу.
5. *Тиран:* система, которая отвергает любую операционную систему, не «авторизованную» производителем.

Пользователи проприетарного ПО беззащитны перед этими формами злоупотреблений. Избежать их можно, настаивая на свободном (уважающем свободу) ПО . Поскольку свободное ПО контролируется его пользователями, у них есть довольно хорошая защита от вредоносных функций ПО.

Последние добавления

- 2022-05

  Apple маркирует различные сторонние файлы и программы как «поврежденные» , не позволяя пользователям открывать их и подразумевая, что программное обеспечение из сторонних источников опасно. Хотя эти ограничения можно обойти, они нарушают свободу пользователей выполнять вычисления так, как они хотят. В большинстве случаев цель предупреждений, таких как «поврежденный», — напугать пользователей, чтобы они продолжали использовать фирменные программы Apple без веской причины.

- 2025-03

  Microsoft ужесточает цепи, которые заставляют пользователей Windows входить в учетную запись Microsoft [*], таким образом идентифицируя себя. Мы подозреваем, что это намеренная стратегия, чтобы избежать одновременного возникновения большого сопротивления: оставить возможности для избегания идентификации, а затем постепенно закрыть их.

  Хватит!

  [*] Почему «использует»? Потому что запуск Windows — это не вы используете Windows, это Windows использует вас.

- 2024-07

  Компания, производящая «умную» люльку под названием Snoo, заблокировала самые передовые функции Snoo за платным доступом . Это неожиданное изменение в основном затрагивает пользователей, которые получили устройство в подарок или купили его подержанным, предполагая, что все эти функции будут доступны им, как и раньше. Это еще один пример обманного поведения разработчиков проприетарного программного обеспечения, которые пользуются своей властью над пользователями, чтобы менять правила по своему усмотрению.

  Еще одной вредоносной функцией Snoo является тот факт, что пользователям необходимо создать учетную запись в компании, которая таким образом получает доступ к персональным данным, местоположению (SSID), журналу устройства и т. д., а также к заметкам, сделанным вручную, об истории ребенка.

- 2018-07

  Nintendo приложила немало усилий, чтобы помешать пользователям устанавливать стороннее ПО на свои консоли Switch . Теперь это полноценные джейлы.

- 2025-02

  Apple прекратила предлагать сквозное шифрование iCloud в Великобритании после того, как правительство Великобритании потребовало всемирный доступ к зашифрованным данным пользователей . Это еще одно доказательство того, что хранение собственных данных «в облаке» подвергает их риску.

Больше товаров...