Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Как работает антивирус
- Рекомендации

Что такое антивирус?

Обзор

Антивирус – это программа для защиты компьютера или мобильного устройства от вредоносных программ. Термин «вредоносные программы» включает в себя все возможные виды опасных программ, таких, как вирусы, черви, трояны и вирусы-шпионы. То есть термин состоит из двух ключевых слов: «вредоносный» и «программы». В случае заражения вашего компьютера вредоносными программами, кибер преступник может перехватывать каждое нажатие клавиши, красть ваши документы или сможет атаковать другие компьютеры с помощью вашего. Вопреки некоторым мнениям, абсолютно любая операционная система может быть инфицирована, включая MAC OS X и Linux.

Автор выпуска

Джейк Уильямс – основатель компании Rendition Infosec (**www.renditioninfosec.com**), сертифицированный инструктор и автор курса Института SANS. Ведет записи в Twitter как **@MalwareJake** и в своём блоге **malwarejake.blogspot.com**.

Антивирус можно приобрести отдельно или в составе пакета безопасности программного обеспечения. Проблема в том, что антивирус не всегда успевает идти в ногу со злоумышленниками, которые постоянно разрабатывают и выпускают новые вредоносные программы. Ежедневно выпускается такое количество новых вредоносных программ, что ни один антивирус не может их все обнаружить и обезвредить. Вот почему важно понимать, что антивирус не может защитить ваш компьютер от всех существующих вредоносных программ. Чтобы понять, почему так, давайте рассмотрим, как он работает.

Как работает антивирус

Можно выделить два направления, по которым работают антивирусы: поиск по известному коду (сигнатуре) и по поведению. Поиск по базе сигнатур работает как иммунная система человека. Антивирус сканирует компьютер в поисках признаков или, так называемых, сигнатур вирусов. Этот принцип основывается на обращении к словарю известных вредоносных программ, если что-то соответствует образцу в словаре, программа пытается это нейтрализовать. Этот подход требует постоянных обновлений, например, как иммунной системе человека требуются прививки от новых штаммов вируса гриппа. Антивирус может защитить только от того, что он признает вредным. Проблема заключается в том, что кибер преступники разрабатывают новые вредоносные программы так быстро, что разработчики антивирусов не успевают за ними угнаться. В результате чего

Что такое антивирус?

всегда есть новые варианты вредоносных программ, которые могут обойти антивирус, даже если его регулярно обновлять.

Обнаружение по поведению заключается в том, что антивирус ищет не вредоносные программы, а наблюдает за поведением программ, установленных на вашем компьютере. Когда программа работает подозрительно, например, пытается получить доступ к защищенному файлу или изменить другую программу, то антивирус замечает эту активность и предупреждает вас о ней. Такой подход обеспечивает защиту от абсолютно новых вредоносных программ, которых нет ещё в словаре. Проблема данного подхода в том, что антивирус может генерировать ложные предупреждения. Пользователю не всегда легко понять, что стоит принять, а что нет, и со временем компьютер станет уязвим. Вы можете нажимать кнопку «Принять» на каждое предупреждение, тем самым лишать компьютер защиты. Более того, вредоносная программа может запуститься раньше, чем антивирус её обнаружит и определить, кто проявляет активность: вирус или антивирус, будет невозможно.

антивирус является важной частью безопасности, но он не может обнаружить и предотвратить все атаки. Никакие технологии не могут защитить вас лучше, чем вы сами.

Антивирус является важной частью обеспечения безопасности компьютера или мобильных устройств, поэтому мы рекомендуем его установить и активно использовать. Но всегда следует помнить, что как бы хорошо не работал антивирус, он не в состоянии защитить вас от всех видов вредоносных программ. Помните, что только вы можете защитить себя лучше любой технологии.

Рекомендации

1. Приобретайте антивирусы только у известных производителей и из надежных источников. Очень часто кибер преступники под видом антивируса распространяют вредоносные программы.
2. Убедитесь, что пользуетесь последней версией антивируса, он регулярно обновляется, настроено автоматическое обновление и годовая подписка оплачена. Если какое-то время ваш компьютер был выключен или отключен от Сети, необходимо сразу обновить антивирус при включении или подключении к Интернету. Не откладывайте эти важные обновления.
3. Убедитесь, что антивирус автоматически сканирует портативные устройства, такие, как USB-карты, в режиме реального времени.

Что такое антивирус?

4. Всегда обращайте внимание на предупреждения антивируса. Большинство предупреждений содержат подробную инструкцию о последующих действиях. Если вы получили предупреждение на рабочем компьютере, немедленно обратитесь в Службу Поддержки или к непосредственному руководителю.
5. Никогда не отключайте и не удаляйте антивирус только потому, что он замедляет работу компьютера, блокирует сайты или установку приложений или программ. Это подвергает вас большой опасности и может привести к серьёзным последствиям. Если проблемы возникают на рабочем компьютере, обратитесь в Службу Поддержки. Если затруднена работа на личном компьютере, свяжитесь с разработчиком антивируса, посетите их сайт для получения дополнительной информации или замены антивирусной программы на другой продукт.
6. Не устанавливайте одновременно несколько антивирусов на ваш компьютер, это может привести к конфликту программ и снижению безопасности.
7. Научитесь распознавать предупреждения вашего антивируса. Кибер преступники могут размещать на сайтах очень реалистичные поддельные «предупреждения», которые предлагают «помочь» обезвредить вирусы на вашем компьютере. Если вы перейдёте по ссылке или нажмёте кнопку, то можете на самом деле заразить свой компьютер.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

Сравнение антивирусных продуктов:	http://www.av-test.org/en/
Социальная инженерия:	http://www.securingthehuman.org/ouch/2014#november2014
Фишинг: атаки по электронной почте:	http://www.securingthehuman.org/ouch/2013#february2013
Меня взломали, что делать?:	http://www.securingthehuman.org/ouch/2014#may2014
Антивирусная программа:	https://ru.wikipedia.org/wiki/Антивирусная_программа
Обнаружение, основанное на сигнатурах:	https://ru.wikipedia.org/wiki/Обнаружение,_основанное_на_сигнатурах

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова

