Автор: Максим
08.02.2010 14:58 - Обновлено 20.05.2011 11:30

Цель данной статьи - рассказать пользователям о более эффективных методах противодействия злоумышленникам, чем использование антивирусных программ.

С распространением компьютерной техники и массовым подключением к сети Интернет очень остро встаёт вопрос о защите информации. Высокие технологии создавались, чтобы облегчить труд человека, сделать его отдых более продуктивным и интересным, но к сожалению, человеческая природа такова, что некоторые люди стали использовать технологии для извлечения личной выгоды путём нанесения ущерба информационным системам или воровства информации у большого количества людей. С развитием технологий методы создания вредоносных программ упростились на столько, что сейчас они доступны даже школьнику. Практически сразу с появлением вредоносных программ появились и программы противодействующие им: антивирусы, спам фильтры, файрволлы и брендмауэры, однако ни одна программа не может обезопасить Вашу информацию на 100% т.к. новые вирусы или вредоносные программы, как правило не распознаются антивирусом, пока фирма разработчик антивируса не узнает о существовании новой "заразы", не выпустит обновление для своих программ, а пользователи не скачают его из Интернет и не установят.

Сейчас противодействие вредоносным программам - это хорошо отлаженная индустрия с миллиардными доходами, а потому в массовую культуру активно насаждается миф о том, что антивирусная программа - это единственный и самый эффективный способ противодействия злоумышленникам, и каждый компьютер или даже каждое интеллектуальное электронное устройство (например, сотовый телефон) должны содержать антивирусную программу. Но данное положение дел выгодно только производителям антивирусов, так как использование этих программ для обычных пользователей несёт в себе негативные скрытые особенности

Основные негативные аспекты внедрения антивирусных программ для пользователей:

- **Рост затрат на программное обеспечение и техническую поддержку.** Как правило, антивирусные программы имеют весьма высокую стоимость владения, особенно учитывая тот факт, что зачастую их эксплуатация из-за карантинных мер вызывает определённые технические проблемы в системе, блокирует работу полезных программ, и требует обращения к специалистам для правильной настройки антивируса.

- **Снижение производительности компьютера.** Все антивирусные программы сканируют информацию на жёстком диске, а также все запускаемые программы, что приводит к существенному падению производительности компьютера, значительному

увеличению времени запуска программ и такому неприятному эффекту, который часто именуют "тормозит".

- **Неоправданное усложнение эксплуатации компьютера.** Несмотря на то, что антивирусные программы создавались чтобы автоматизировать и упростить деятельность по обнаружению и удалению вредоносных программ, как правило их эксплуатация происходит в полуавтоматическом режиме. Пользователь вынужден выбирать варианты действий на подозрительную активность, что вызывает непонимание у неподготовленных пользователей, а также неоправданную остановку работы, кроме того не исключена возможность выбрать неверный вариант, что в конечном итоге приведёт к невозможности использования какой-нибудь полезной программы.

В тоже самое время есть и другие методы защиты информации, самый эффективный из них - это получение необходимых знаний о защите информации. Прежде всего необходимо сказать, что массовое распространение вирусов характерно только для самой популярной программной платформы - Windows, другие платформы на порядки в меньшей степени подвержены действию вредоносных программ.

Чрезвычайно эффективным методом противодействия является использование отличной от Windows программной платформы, например свободной платформы на основе ядра Linux.

Дело в том, что 99% всех существующих вредоносных программ могут успешно работать только в системах Windows. Используя операционную систему, отличную от Windows, Вы исключаете возможность работы подавляющего большинства вредоносных программ без использования антивирусов. Вирусописателям потребуются годы, чтобы освоить новую платформу и достичь того же уровня развития вирусов, который мы наблюдаем сейчас на Windows, это действительно сложная задача, так как Linux платформа в значительной степени более устойчива к угрозам информационной безопасности и проверена годами эксплуатации на подавляющем большинстве серверов в сети Интернет. При использовании свободной платформы Linux, помимо повышения информационной безопасности вы получаете ещё и значительную выгоду от экономии средств на покупку ОС Windows и антивирусной программы.

Простые правила

1. Не устанавливайте и не запускайте программы, предназначение которых Вам неизвестно, функциональность которых никем не проверена. Программы (исполняемые файлы) в Windows имеют расширения имени файла *.exe *.com *.bat *.cmd *.vbs *.js. Где * обозначает любые символы в любом количестве.
2. Обращайте внимание на расширение имени и размер тех файлов, которые Вы открываете. Документы, видео, картинки или музыка не могут иметь расширение, как у исполняемого файла - это обман с целью стимулировать выполнение вредоносной программы.
3. Не скачивайте программы и документы (даже если их предназначение Вам известно) с сомнительных Интернет сайтов, особенно это касается порталов по распространению нелегальных копий программ, и сайтов порнографического содержания.
4. Не пользуйтесь браузером Internet Explorer для просмотра сайтов, чья репутация не проверена или вызывает сомнения. Этот браузер в наибольшей степени подвержен атакам злоумышленников.
5. Следите за обновлениями безопасности Вашей системы и браузера, своевременно обновляйте программы.
6. Периодически делайте резервную копию наиболее важной информации на Вашем компьютере, используя CD/DVD диски, FLASH накопители или внешние жёсткие диски. Храните резервные копии отдельно от компьютера.
7. **Используйте парольную защиту Вашей учётной записи, и шифрование конфиденциальной информации.** Не разглашайте Ваш пароль или секретный ключ

Простые настройки системы

1. **Отключите автозапуск программ с CD/DVD/FLASH/HDD и сетевых дисков.** Эта опция доступна в свойствах каждого диска программы "Мой компьютер"

Следуя приведённым выше рекомендациям Вы в значительной степени повысите информационную безопасность Вашего компьютера и с высокой долей вероятности исключите проникновение злоумышленников и вредоносных программ.