Почему массы не слишком высокого мнения о рынке ИТ-безопасности (информационных технологий)? Не так давно каждый крупный новостной источник регулярно сообщал о проблемах компьютерной безопасности. В 2001 году весь мир узнал о Code Red, Nimda и Code Red II. Но за прошедшие с тех пор более 7 лет уровень освещения вопросов компьютерной безопасности неуклонно снижался. Со времени публикации Zotob в начале 2005 года (которая была незначительной по сравнению с публикациями 2001 года), ничто и близко не приблизилось к уровню охвата, даже несмотря на то, что штормовой червь был гораздо более распространенной проблемой. На самом деле, это было правдой, когда я начинал писать эту книгу, но, когда я заканчиваю ее, червь Conficker за последние полгода заполонил все публикации о технологиях. Все, кто работает в сфере безопасности, слышали о нем, и многие специалисты в области информационных технологий тоже. Я опросил об этом друзей и родственников и обнаружил, что люди, которые хорошо следят за новостями, не знают об этом, а это значит, что если они и видели статью о Conficker, то, скорее всего, пропустили ее. Даже мои друзья-техники, похоже, равнодушны к этому, а многие из тех, кому это было бы небезразлично, уже давно перешли на Mac.

Сегодня технический мир может много слышать о проблемах безопасности, но мир в целом редко об этом слышит. Это не из-за отсутствия проблем с безопасностью. Конечно, количество вредоносных программ в последние несколько лет растет по экспоненте, поскольку на вредоносных программах можно заработать много денег. Почему при такой масштабной экономике вредоносных программ эта тема не является широко распространенной? Что ж, пресса не сообщает об этом, потому что людям уже все равно, и чем меньше пресса сообщает, тем меньше людей это волнует, создавая приятную нисходящую спираль невежества. Тем не менее, существует множество других факторов, которые мешают людям интересоваться этой темой:

Вредоносное ПО любит оставаться скрытым

Если бы вы были заражены, то на какое-то время ваш компьютер, вероятно, стал бы работать невероятно медленно, а повсюду появлялись бы тонны рекламы. Авторам вредоносных программ не потребовалось много времени, чтобы понять, что они не смогут заработать на пользователях столько денег, если заражение было очевидным и пользователь заплатил за его очистку. В наши дни вредоносные программы обычно пытаются делать свое дело незаметно. Даже когда вредоносное ПО размещает рекламу, оно обычно не перегружает вас ею. Время от времени вы можете получать всплывающие окна, но их не так много. Или же вы можете незаметно заменить законную рекламу на ту, которую хотела бы показывать вредоносная программа. В результате люди не замечают многих случаев заражения, поэтому у потребителей складывается впечатление, что либо их программное обеспечение для обеспечения безопасности выполняет свою работу, либо проблем просто нет.

Продукты для обеспечения безопасности не являются приоритетными.

Давайте предположим, что решения для обеспечения безопасности настольных компьютеров на самом деле работают хорошо (хотя это и не очень хорошее предположение). В случае с традиционными AV-продуктами, возможно, продукт работает хорошо, предотвращая запуск вредоносных программ на вашем компьютере. Обычный потребитель никогда не увидит, как работает AV-программное обеспечение, и не отдаст ему должного.

Последствия были не так уж плохи

Многие потребители ожидали интернет-апокалипсиса, когда у значительной части людей, которых они знали, будут опустошены банковские счета и украдены их личные данные. Какое-

то время люди боялись заниматься коммерцией в Сети. Люди, которые больше всего боялись, просто отказались покупать товары онлайн. Все остальные были несколько утешены, потому что основную ответственность будут нести компании, выпускающие кредитные карты. Кроме того, такие вещи, как кража карты, не только не устраняются, но и когда у кого-то крадут личные данные, не всегда ясно, что это было сделано на компьютере.

Например, если вы находитесь в США, и кто-то украл номер вашей кредитной карты, более вероятно, что кража произошла в ресторане, где кто-то записал данные вашей карты, когда он или она отнесли ее в подсобку, чтобы стереть.

Эта история скучна

Для обычного человека Code Red, Nimda и им подобные - это примерно одна и та же история. Проблемы компьютерной безопасности не попадают в заголовки, потому что слишком многое напоминает предыдущий инцидент. Да, могут быть незначительные различия в том, кто подвержен заражению, что делает вредоносное ПО и насколько быстро оно распространяется, но особенно если вы (как обычный человек) предполагаете, что не подвергаетесь особому риску, в конечном итоге вы просто перестанете читать эти истории, и репортеры будут вынуждены перестаньте их писать — репортаж - это бизнес, и деньги приходят от того, что вы следите за историями, которые люди хотят прочитать.

Индустрия безопасности не слишком надежна

Люди не будут обращать на это внимания в мире, где все, кажется, “знают”, что, например, AV-решения “в большинстве случаев не работают” и что они “замедляют работу вашего компьютера”. Есть ли правда в таких вещах (а она есть), индустрия безопасности не знает. не пользуется большим доверием (я не могу сказать вам, сколько раз люди, честно говоря, спрашивали меня, пишет ли McAfee вирусы для того, чтобы их можно было обнаружить). Поэтому, если история ориентирована на поставщика, она будет не слишком правдоподобной.

Давайте посмотрим правде в глаза: компьютерная безопасность - это огромная проблема для всего мира. Независимо от того, существует ли серьезная проблема (а она есть), для людей это, похоже, не имеет значения. Это означает, что широкая общественность в значительной степени не информирована, и это имеет некоторые последствия для отрасли:

• Потребители не видят разницы между продуктами для обеспечения безопасности. Обычно они ожидают, что один продукт будет выполнять все функции.

• Потребители не готовы платить много за продукты для обеспечения безопасности. Несмотря на то, что они рассчитывают купить один продукт, который выполняет все функции, они чувствуют, что их обкрадывают, вынуждая покупать полноценные комплекты, в которых они не понимают, в чем реальная разница между функциональностью начального уровня и функциональностью премиум-класса. Воспринимаемая ценность невелика, и люди ожидают, что получат много функций, которые они не используют.

Похоже, что люди в целом считают, что AV - это “must have” (особенно в Windows), но не очень уверены в его способности защитить их.

Одним из интересных следствий этого является то, что многие люди не обращают внимания на то, есть ли у них на самом деле работающий AV или нет. Многие люди получают свой AV-плеер от крупного производителя в качестве предустановки OEM (производителя оригинального оборудования) (это означает, что он поставляется вместе с ПК, который они купили у Dell, HP, Gateway или у кого-либо еще). Они предполагают, что получают его бесплатно, пожизненно.

Однако большинство из этих предустановок рассчитаны на ограниченное время, обычно не более чем на год. Когда у пользователей заканчивается бесплатный период, они часто не продлевают его. Для этого есть много причин, но обычно люди игнорируют назойливые всплывающие окна на панели задач, а затем либо не замечают, когда истекает срок действия защиты, либо забывают об этом.

На самом деле простых решений для улучшения общественного восприятия не существует. Я думаю, что защита прав потребителей быстро теряет свою ценность, особенно при разумном распространении бесплатных AV-решений, таких как AVG, Avira и Avast (извините, в мире с открытым исходным кодом ClamAV не регистрируется). Несмотря на то, что у поставщиков бесплатных видеоигр плохие бренды, у них достаточно пользователей, и это говорит о том, что люди начинают переходить от решений, основанных на бренде, к решениям, основанным на цене. Это не значит, что я считаю, что лучшие бренды обязательно производят лучшие продукты, просто сотрудничество с крупным брендом - это кратчайший путь к проведению исследований. Потребители предполагают, что крупный бренд будет достаточно компетентным, иначе он не был бы успешным.

Нет, я думаю, что путь будет долгим и трудным. Существует множество проблем, многие из которых я собираюсь рассмотреть в последующих главах.