В июле 2008 года появилось сообщение, в котором утверждалось, что если подключить незащищенный компьютер с Windows XP к Интернету и ничего больше не предпринимать, он будет заражен в среднем за четыре минуты. Типичная рекомендация для предотвращения подобных проблем - запустить брандмауэр в вашей сети и как можно быстрее установить все последние обновления. Все это звучит пугающе, но не волнуйтесь, этот отчет - полная чушь. Это просто мусор, используемый для распространения страха, маркетинговый инструмент для организации, производящей эти цифры (в данном случае это SANS, компания, которая проводит обучение и сертификацию по безопасности и проводит конференции по безопасности; такая пресса может укрепить ее репутацию и заставить людей покупать ее услуги). Это правда, что существует множество автоматизированных программ, которые случайным образом сканируют Интернет в поисках уязвимых систем для заражения. Это неправда, что вы, скорее всего, будете заражены.

Основная причина, по которой это полная чушь, заключается в том, что в Windows XP (начиная с пакета обновления 2) уже есть брандмауэр, который защищает вас. Если вы устанавливаете что-то более старое, чем Windows XP с пакетом обновления 2 (который вышел в конце 2004 года), вам придется беспокоиться о том, есть ли в сети что-то, защищающее вас. Хотя во многих случаях это так, независимо от того, знаете вы об этом или нет.

Ваш интернет-провайдер может предотвращать попадание нежелательного интернет-трафика на ваш компьютер. Возможно, на вашем беспроводном маршрутизаторе или кабельном/DSL-модеме по умолчанию включен брандмауэр. И, вероятно, на вашем маршрутизаторе/модеме по умолчанию включен NAT (преобразование сетевых адресов). NAT защитит вас от внешних угроз, даже если вы используете самую старую версию Windows XP или даже Windows 95. Эти технологии защищают вас, потому что они препятствуют доступу трафика из внешнего мира к программному обеспечению, работающему на вашем компьютере. Это программное обеспечение потенциально уязвимо. Брандмауэр работает как своего рода привратник. Он выборочно выбирает, какой трафик пропускать, а какой нет. Брандмауэр, установленный в вашем беспроводном маршрутизаторе или кабельном/DSL-модеме, вероятно, будет иметь политику, которая сводится к следующему:

Если из внешнего мира поступает новый запрос на подключение, отклоните его. Если новый запрос на подключение поступает изнутри брандмауэра, разрешите его, а также любой трафик в последующем диалоге.

Это означает, что вы можете подключиться к веб-серверу из своего браузера, но если на вашем компьютере запущен веб-сервер, никто из внешнего мира не сможет подключиться к нему. NAT работает по-другому, но имеет тот же базовый результат. Вместо того, чтобы быть фильтром как таковым, он позволяет множеству компьютеров совместно использовать один IP-адрес (как правило, это все, что может предоставить вам ваш интернет-провайдер). Этот адрес обычно не разрешает никаких входящих подключений. Это возможно, но вам придется настроить его вручную. Вместо этого все пользователи сети получают адрес, который работает не в Интернете, а только в локальной сети.

Устройство NAT принимает запросы на исходящее подключение, создает видимость того, что они поступают с IP-адреса, предоставленного вашим провайдером, затем принимает полученные данные и пересылает их на любой компьютер, который инициировал подключение. Эти технологии чрезвычайно затрудняют доступ к вашему компьютеру без вас кому-либо из внешнего мира. делать что угодно. Как правило, вам приходится делать что-то, что приводит к вашему заражению. Возможно, вы заходите на веб-сайт, который использует уязвимости в системе безопасности вашего веб-браузера или обманным путем заставляет вас загрузить что-то вредоносное. Возможно, вы получаете электронное сообщение, в котором используется

уязвимость в системе чтения электронной почты или просто обманным путем заставляете вас установить его. В любом случае, вы несете ответственность за инициирование исходящего соединения в первую очередь (даже если программа чтения электронной почты периодически устанавливает это соединение от вашего имени).

Брандмауэр Windows выполняет ту же роль, что и сетевой брандмауэр, но находится на вашем отдельном компьютере, а не на кабельном модеме или DSL-маршрутизаторе. Это особенно полезно в крупной корпоративной сети, где кто-то другой мог заразиться, и эта зараженная машина в противном случае могла бы иметь доступ к какой-либо уязвимой программной службе, запущенной на вашем компьютере. Но существует больший риск заражения в локальной сети, поскольку люди, как правило, более либеральны в отношении того, что разрешено в локальной сети. Средства автоматической связи, совместного использования файлов и принтеров широко распространены, и брандмауэры обычно не блокируют такие действия по умолчанию.

Очевидно, что существует множество механизмов предотвращения, которые обеспечивают безопасность вашего компьютера. Даже если это происходит только на вашем компьютере, вы, вероятно, в хорошей форме. Так почему же SANS говорит то, что не похоже на правду? Во-первых, SANS действительно что-то измеряет. Он публикует ежедневные цифры (хотя на момент написания этой статьи данные заканчиваются 16 ноября 2008 года). Число колеблется. Например, 16 ноября 2008 года SANS заявила, что компьютер с Windows проработает чуть менее 100 минут до заражения, если не будет использовано какое-либо устройство сетевой защиты.

SANS не публикует свою методологию. Я предполагаю, что она работает под управлением версии Windows XP, выпущенной до выпуска 2004 года с пакетом обновления 2. Меня не удивит, что у компьютера, на котором запущено это программное обеспечение, возникнут проблемы, если вы выложите его в Интернет в чистом виде. Но хотя люди могут давать вам разумные советы (да, с таким же успехом можно было бы установить брандмауэр, и да, обновлять свое программное обеспечение, особенно то, что вы используете, например, свой веб-браузер), когда они делают пугающие заявления, не верьте шумихе без веских доказательств.