**Страшные сказки о безопасности Windows и Интернет**

Ардынцев Виталий

Безопасность в Интернет традиционно рассматривается на уровне приложений. То есть, весь анализ сводится к фразам типа "а что будет если послать письмо в телеконференцию и указать свой истинный адрес e-mail", или, а что будет если зайти на такой то сайт там заполнить форму, указав там полный номер своей кредитной карточки". Естественно последствия вполне очевидны и понятны всем. В первом случае spam (мощный поток рекламных писем на ваш e-mail адрес), во втором утечка денег. Тривиально! Тривиальны и рекомендации - не заполняйте формы и не указывайте ваш истинный email в прямой форме, а слегка замаскируйте его. Пишите свой адрес примерно в таком виде dima"no\_spam"@bigfot.com. Естественно, человек при написании ответа удалит "no\_spam". Интересно, что же рекомендуют делать в солидных московских компьютерных журналах (Компью-Терра), если вы всё-таки получили spam? Очень смешно, но рядовому пользователю предлагается до тонкостей изучить протоколы прохождения рекламных сообщений и, используя многочисленные хитрые методы и программы определить некий IP (тёмный лес для обычного человека), а по нему, опять же с применением сложных методов имя провайдера, через которого посылается на вас spam. Скорее всего это будет иностранная фирма с сотнями тысяч или даже миллионами пользователей, занимающихся в том числе и рассылкой рекламы и, соответственно, с огромным потоком жалоб. Далее в Компью-Терре рекомендуется послать этому провайдеру жалобу. Ха-ха-ха! Результат очевиден - вашу жалобу рассмотрят через несколько лет, может быть. Да, в этом вопросе Питер обогнал Москву. У нас практически все провайдеры в той или иной форме берут борьбу со spam на себя. Например, провайдеры предоставляют специальный тариф бесплатного приёма неограниченного объёма электронной почты при небольшой ($5) фиксированной месячной плате. Многие провайдеры по первой просьбе устанавливают так называемые фильтры, блокирующие поступление e-mail сообщений с определённых адресов. Для этого пользователю достаточно переслать образец нежелательной почты своему провайдеру и попросить поставить фильтр. Вот настоящее решение проблемы, доступное любому, даже начинающему пользователю Интернет в Петербурге!

Нигде и никогда не обсуждался вопрос безопасности интернет на "идеологическом" уровне. А ведь с появлением Winternet 98 (Windows 98) именно идеологическая сторона становиться наиболее интересной. Windows 98, на мой взгляд, имеет принципиально новую черту. Теперь каждая отдельная копия этой операционной системы на каждом конкретном ПК в момент подключения к Интернет становиться частью огромной единой глобальной операционной системы Microsoft. Самым безобидным или даже незначительным побочным эффектом является автоматическое обновление (изменение?) внутренних частей Windows 98. А главным становиться то, что в момент подключения к Интернет фактически ВСЁ содержимое жёсткого диска любого компьютера становится доступным Микрософт. Больше нет никаких сдерживающих барьеров! Все протоколы, включая TCP/IP, реализованы одной и той же фирмой. Фактически уже не важно TCP/IP или XXX/XX протокол использовался для подключения к Интернет. Важно, что этот протокол реализован одной фирмой. Все пароли фактически хранятся в теле одной глобальной операционной системы, части которой расположены на ПК с Windows 98, а главная часть во главе со всемирным системным администратором с неограниченными правами доступа (а кто или что может его ограничить ?!) к любому компьютеру в лице пока кажущегося безобидным Билом Гейтсом очевидно в штаб-квартире Microsoft.

Одно это должно вызывать по крайней мере чувство тревоги и озабоченности. Как же это выглядит на практике? А вот так! Новый Большой Брат (Microsoft) непрерывно круглосуточно сканирует содержимое жёстких дисков десятков или даже сотен миллионов компьютеров по всему миру (и ваш домашний ПК тоже, если у вас установлена Windows 98) через интернет, извлекает и скачивает информацию о версии операционной системы, об аппаратуре (звуковой и видео карте, модеме, жёстком диске и т.д.) и программном обеспечении, установленном на ПК, анализирует и, в случае, необходимости автоматически через Интернет обновляет части операционной системы, драйвера и другое программное обеспечение. А автоматически означает, что как только вы подключаетесь к Интернет (причём совершенно неважно через какого провайдера) первым делом операционная система вашего компьютера связывается с Большим Братом и докладывает ему всё о состоянии вашего ПК и программного обеспечения. Затем, по приказам Большого Брата производятся обновления или изменения файлов. Причём всё это происходит в фоновом режиме, незаметно для вас. И это не фантастика - это реальность уже сегодняшнего дня! Многие скажут, что такая система очень удобна как для Microsoft, так и для конечного пользователя. Но благими намерениями вымощена дорога в ад... Видимо первым делом Microsoft воспользуется тотальным контролем компьютеров через Интернет для борьбы с нелегальными пользователями (пиратами) программных продуктов. Сделать это можно очень просто. Например, при первом же подключении к Интернет автоматически проверяются серийные номера, регистрационные имена и другая лицензионная информация программных продуктов на ПК и если верификация не проходит, то начинается удаление всех нелицензионных файлов, включая и саму операционную систему (если это пиратская копия). Короче говоря делается низкоуровневое форматирование жёсткого диска. Возможен и другой более хитрый вариант. Большой Брат может проанализировать содержимое жёсткого диска вашего ПК на предмет обнаружения информации о вашем местожительстве, телефоне, адресов людей с которыми вы переписываетесь, ваших паспортных данных (например, у вас на ПК хранится текст трудового соглашения с вашим текущим работадателем) и другой конфиденциальной информации. Затем эта информация может быть переслана (опять же по Интернет) в местные компетентные, органы (милицию и т.д.) по борьбе с нелегальным копированием программного обеспечения.

Кроме борьбы с компьютерными пиратами открываются и другие грандиозные возможности. Причем цели могут быть как благородными, так и преступными. Важен сам факт создания Всемирной Информационно-Программной Империи. Пока во главе её находится по большому счёту довольно безобидный человек. Билл Гейтс всё же не похож на Гитлера или Сталина. Но к старости характер обычно портится. Да и не исключена возможность захвата легальным (покупка 51% акций) или нелегальным (убийство Билла Гейтса) способом Microsoft мафией, крупной финансово-промышленной или политической группой (а если коммунистами или фашистами?). Думаю, что и для могущественных специальных службы типа Моссад, КГБ или ФБР/ЦРУ Microsoft является невероятно привлекательным объектом. И тогда может случится, что при включении любого компьютера первым делом надо будет вводить в качестве пароля номер членского билета какой-либо партии (КПРФ?) и номер платёжки об уплате членских взносов. А затем последует обязательное промывание мозгов типа "пятиминутки ненависти", ну и далее смотри по тексту известной книги. Ещё раз повторюсь, Всемирная Информационно-Компьютерная Империя (после появления Windows 98) стала реальностью. Единственное, что пока спасает нас от апокалиптического развития событий это незлобливый и без политических амбиций характер Билла Гейтса. Очевидно, что монополия не должна быть всемирной. Одним из разумных выходов может быть опубликование всех исходных текстов Windows 98, что позволило бы убедиться в отсутствии "информационных бомб" и "электронных шпионов" в этой операционной системе-монополисте.

Я провел небольшой опрос среди как "домашних" пользователей персональных компьютеров, так и профессиональных системных администраторов крупнейших провайдеров Интернет Петербурга и других городов. Выяснилось, что рядовые пользователи с трудом верят в такие штуки. Основной их аргумент (довольно смешной для многозадачной распределённой операционной системы) звучит примерно так: "Все же для того, чтобы операционная система начала шарить по диску, надо все же нажать какую-то кнопку". В этом сладостном заблуждении и пребывают 95% человечества. Конечно нажимать ни на что не надо. Теоретически (это подтвердит любой начинающий программист) единственная кнопка требующая нажатия - это кнопка "включить питание"! После этого на вашем компьютере загрузиться некая программа под названием Windows такой то версии (если вы не исхитрились установить предварительную загрузку Нортона Командера, а 90% людей в мире давно уже не пользуют досовских программ). Эта программа Windows теперь содержит в себе всё необходимое для выходя в Интернет и проделки всех необходимых фокусов. Ещё недавно Windows был отделён от Интернета стеной программного обеспечения от независимых фирм, что и служило некоторой гарантией безопасности (в той мере в какой вы доверяли этим фирмам). Теперь Windows это нечто, являющееся частью огромной распределённой системы, очень похожей на нейронную(!) сеть с управляющим центром в штаб-квартире Microsoft. Отдельные нейроны(ПК) этой сети соеденены между собой через Интернет. (Не читали случаем полунаучный опус Станислава Лема на эту тему? Он утверждает, что когда вычислительная мощность этой виртуальной нейронной сети достигнет некоторой пороговой величины, сопоставимой с мощностью 15 миллиардной нейронной сети головного мозга человека, произойдёт качественный скачок (диалектика...) и самоорганизация сети в искусственный интеллект). Совершено очевидно, что если "звонилка" и tcp/ip являются частью самой операционной системы, то уже ничто не может остановить Windows, если она "захочет" дозвониться до провайдера и подключится к Интернет (пусть даже и по международному номеру штаб-квартиры Microsoft) и проделать всё что я описывал раньше. Для понимания этого даже не надо быть специалистом, достаточно просто здравого смысла. И для меня скорее загадка не в том как это сделать, а почему Билл Гейтс или какой-нибудь зловредный программист из многих десятков тысяч работающих в Микрософт не сделали этого до сих пор (а может уже...). Кстати один мой знакомый ГУМАНИТАРНЫЙ журналист самостоятельно осваивая домашний компьютер и Интернет некоторое время дозванивался до своего питерского провайдера через 8 (межгород) пока не получил телефонный счёт...Оказывается по умолчанию его Windows 98 "звонилка" выходила на межгород! Вот так то... наводит на размышления...

Совершенно другое отношение к моим взглядам на проблему безопасности в Интернет высказали профессиональные системные администраторы провайдеров Интернет. Все они согласны с тем, что технически у Глобального Системного Администратора (Microsoft) есть реальная возможность доступа к любым данным на локальных персональных компьютерах под управлением Windows 98. С другой стороны они выдвинули и несколько серьёзных возражений. Рассмотрим их подробнее. Большинство Интернет профессионалов отмечает, что скачивание пользовательских файлов с локальных ПК приведёт к слишком заметным увеличениям трафика для Dial-UP клиентов. А это - зацепка. Увеличение будет, но возможно очень незначительное. Microsoft не надо скачивать или закачивать мегобайты за один раз. Во первых, процесс будет растянут во времени на несколько дней или недель. То есть большой файл будет закачиваться постепенно, маленькими кусками. Во вторых, для борьбы с программными пиратами достаточно скачать несколько байт регистрационных номеров, что не вызовет заметного увеличения трафика! В третьих, При on-line подключении во время сёрфинга реальная средняя загрузка модема не превышает 30%, а обычно у меня 15%-20%. Надо же и читать то что загружаешь(!), а не только непрерывно скакать с одной страницы на другую. Конечно продвинутые пользователи интернет сначала качают много страниц, а потом в off-line читают, но таких относительно мало и всё равно загрузка модема не достигнет 100% никогда! ТО ЕСТЬ (В СРЕДНЕМ) ВСЕГДА ЕСТЬ СВОБОДНЫЙ КАНАЛ ПЕРЕДАЧИ ДАННЫХ и если его использовать с умом он не будет влиять на ощущения пользователя о скорости соединения с Интернет. В четвёртых, обычный пользователь (а их подавляющее большинство) скорее всего спишет небольшое снижение скорости передачи данных на ухудшение условий связи по телефонной линии! У меня например cps ночью в два раза выше чем днём. Да и в течении дня cps может колебаться от 3000 cps до 700 cps. Так что на снижение скорости пересылки файлов на 10%-15% вообще никто не обратит серьёзного внимания или не придаст этому факту никакого значения! Системные администраторы также высказывают мнение, что в новой версии операционной системы будет возможность отказаться от "удобств" обновления частей операционной системы через интернет и предотвратить таким образом возможность превращения своего ПК в часть глобальной системы. Но как видите опять всё основывается на ВЕРЕ! А правильнее будет сказать, что в Windows 98 есть некая кнопочка или параметр изменив который пользователь будет думать, что он отказался от этих "удобств". А вот РЕАЛЬНО узнать так ли это можно только имея исходники Windows. Очень интересное замечание получил я от одного из Уральских интернет провайдеров. Не знаю шутка это или нет. Привожу текст сообщения дословно: "Заодно Вин-98 загружает во Flash-память модемов (пользователя и провайдера) на время сеанса связи с Интернет секретную прошивку на 115К, чтобы обновление системных файлов происходило действительно незаметно для пользователя. Но нам это на руку - по крайней мере у выделенных клиентов трафик заметно возрастет". Похоже речь идёт о зарождении нового вида вирусов, живущих во Flash-памяти модемов! Такой вирус невозможно удалить даже низкоуровневым форматированием жёсткого диска. В любом случае провайдерам выгодно увеличение трафика клиентов, так что они если и обнаружат странности не будут трубить об этом на каждом углу! Так что отслеживание всяких странностей придётся взять на себя конечным пользователям.

Профессионалы также высказывали мнение, что в сетевой операционной системе Windows 98 предусмотрены меры по управлению правами доступа к содержимому жесткого диска локального ПК. Вот что пишет мне А.Зеленин (www.izhcom.ru): "Хотел сказать - совсем без моего ведома обновлять системные файлы не получится...По крайней мере, я всегда стараюсь знать, что делает моя машина. Обнаружить то, что делает WIN-98 без твоего ведома, как мне кажется, достаточно просто. Вешаешь sniffrra на сегмент и в спокойной обстановке разбираешь логи. Один-два пользователя сделают это и провозгласят всему миру о результатах. Протокол-то он один - TCP/IP и его никто не отменял". В принципе я согласен. Но опять всё это защита от другого пользователя, а не от Глобального Системного Администратора. Допустим, например, пользователь Windows 98 запрещает доступ к некоторым директориям или сегментам жёсткого диска? Но КОМУ он запрещает?! Очевидно, что другому пользователю, но не самой операционной системе и не Глобальному Системному Администратору с АБСОЛЮТНЫМИ правами доступа! Ведь именно сами Windows и контролируют на основе указаний пользователя кому разрешить доступ, а кому нет. Представьте, вы охранник (Windows 98) и вам шеф дал указание не пропускать такого-то человека. А вы взяли да и захотели пропустить его. Ну кто или что вам помешает это сделать?! Только боязнь, что шеф узнает и лишит вас работы (а уволить вас нельзя, других то операционных систем почти "нет") или ваша совесть и добропорядочность. Так что ВСЯ НАДЕЖДА на то, что Билл порядочный человек. То есть опять надо ВЕРИТЬ в Била Гейтса (кощунство?). Но что такое порядочность в условиях капитализма никто толком объяснить не может! А кроме того неужели в огромном АВТОРИТАРНОМ государстве Microsoft нет ДИССИДЕНТОВ или просто плохих парней или, наконец, шпионов от конкурентов или специальных служб и тайных ненавистников самого Microsoft?!

Интересная переписка по поводу этой статьи была у меня с одним из самых авторитетнейших специалистов по Интерент в Петербурге системным администратором нашего крупнейшего провайдера Петерлинк Андреем Дементьевым. Позволю себе привести её полностью:

"Частично всё, что вы описали реально.

1. всякие update'ы действительно могут делаться через Internet

2. это может происходить без Вашего участия, но активна должна быть ваша машина - ПОКА ещё никто не в состоянии опрашивать все компьютеры в мире на предмет чего бы то ни было.

3. Ходят слухи, что Microsoft однажды уже уличили в том, что она при помощи своих программ передает информацию о содержимом жесткого диска пользователя в свое логово (конечно, невозможно передать весь диск, но многое можно сделать и так) Попробуйте поискать через altavista вокруг "регистрация в Microsoft Network" - как раз то, что надо :-)

Но все это никак не связано с мировой катастрофой, которая рисуется в конце. Это - пока нереально :-) Но в общем, вы уже сейчас сильно зависите от Microsoft - вышла новая версия Ворда, не умеющего читать старые файлы, и все ищут перекодировщики :-)"

Далее мой вопрос:

"Встретилась мне такая фраза: в Windows 95 существует странность в реализации TCP/IP, при обращении к порту 3128 с любым запросом система "вешается". Таким образом любой ПК подключенный к интернет может быть подвешен с любого другого ПК подключенного к интернет."

Ответ Андрея Дементьева:

"3128 - нет, он не слушается в Win95. Но есть другие порты - 135, 138,... Пользователи Win95/WinNT обречены на геморрой :-)"

Я довольно быстро нашёл в Интернет несколько программок для "подвески" любого ПК под Windows 95 через Интернет и успешно "подвесил" несколько компьютеров своих знакомых. Получается, я бы сказал, что в Windows реализован некий протокольный айсберг с видимой невооруженным глазом маленькой верхушкой tcp/ip и огромной подводной частью с некому неведомыми и недокументированными возможностями. В наличие недокументированной части не приходится сомневаться. Начиная с самых первых версий операционная система Microsoft ms-dos, а затем и Windows ВСЕГДА позволяла программистам сторонних фирм пользоваться только подмножеством всех доступных функций своих операционных систем. Об этом красноречиво свидетельствуют многочисленные публикации независимых авторов статей и книг с обобщённым названием "Недокументированные возможности ms-dos/Windows", в которых они пытаются хоть в какой то мере приподнять завесу таинственности на секретным "оружием" Била Гейтса. А вот мнение Игоря Коваленко из WEBPlus: "Доля правды состоит в том, что технически возможно существование "люков" в операционной системе и в протокольном стеке. Идеология TCP/IP несколько затрудняет это, но даже при недоступности исходников, это все-же возможно. Техническим препятствием на пути реализации таких люков является существующая децентрализованная природа Internet. Если представить, что все провайдеры действительно "объедятся белены" и установят NT, то это препятствие несколько размоется. Однако слухи о том, что это происходит несколько преувеличены и проблемы все равно останутся. Есть еще и соображения здравого смысла. Такие действия не могут остаться незамеченными, если они начнутся в глобальном масштабе. И тогда надо чтобы либо все пользователи были не очень умными и не обращали внимания, либо MS необходимо обзавестись собственной армией и полицией для укрощения строптивых. Реально же любая попытка подобных действий приведет к краху самой MS, в результате отказа пользователей пользоваться ее продуктами". Однако надо заметить, что отказаться от продуктов Microsoft с каждым годом становиться всё трудней и трудней. И может быть в ближайшем будущем это станет и вовсе невозможным ввиду отсутствия реальной и доступной альтернативы.

А вот мнение Дмитрия Семкина из Nevalink: "Безусловно, приведены разумные доводы. Но при попытке MS или кого-то еще сделать что-то подобное будет затеян очень громкий процесс. Вторжение в частную жизнь в чистом виде. На западе это святое. Скрыть же подобные попытки пока невозможно".

Microsoft изначально стремилась захватить рынок не только операционных систем, но и вообще всего программного обеспечения. План был такой: на первом этапе захватить рынок операционных систем ПК, затем начать постепенно вытеснять с рынка программного обеспечения сторонние фирмы, создавая более надёжное и более функциональное программное обеспечение общего применения, пользуясь преимуществом доступа своих родных микрософтовских программистов ко ВСЕМУ множеству как открытых обществу так и "секретных" недокументированных и иногда практически незаменимых функций. Как мы видим такая стратегия принесла и приносит Microsoft грандиозный успех. Таким образом наличие недокументированных функций и возможностей является ФИРМЕННЫМ СТИЛЕМ Microsoft. Поэтому со 100% уверенностью можно утверждать, что недокументированная часть драйверов сетевых протоколов Windows содержит огромное число всяческих функций для облегчения создания программистами Microsoft систем контроля за локальными персональными компьютерами. Естественно, что доступны они только команде Била Гейтса. В свете выше изложенного я с большим доверием отношусь к сообщения о различных странностях в поведении Windows.

Давайте попробуем догадаться какова же конечная цель Била Гейтса на рынке программных средств и операционных систем? Кажется дело идёт к тому, что на земле останется только ОДНА КОПИЯ одной глобальной сетевой распределенной операционной системы Windows! Все компьютеры по сути превратятся в "сетевые компьютеры", их работа без подключения к Интернет будет функционально сильно ограничена. Все жёсткие диски всех компьютеров будут являться частью ОДНОЙ единой сетевой распределённой файловой системы под управлением одной копии одной глобальной операционной системы Windows. Естественно, все пользователи будут иметь разные права доступа к сетевым ресурсам. Однако не приходится сомневаться, что самый главный системный администратор в лице Microsoft будет иметь доступ абсолютно ко всем ресурсам, включая и любые приватные файлы на любых компьютерах, являющихся частью этой системы. Естественно, что не останется никаких других производителей программного обеспечения кроме Microsoft. И эта монополия принесёт Билу Гейтсу уже просто фантастические деньги. Правда, непонятно зачем ему столько. Так почему же это всё уже не произошло? Очевидно есть сдерживающие факторы. Во первых несмотря на фактическую рыночную монополию на операционные системы для ПК у Microsoft нет ИНТЕЛЕКТУАЛЬНОЙ монополии. Существуют (прозябают?) операционные системы не уступающие или даже превосходящие по некоторым параметрам Windows. Например OS/2 или Linux/UNIX. И если Windows споткнется они мгновенно займут её место. Так что пока Бил Гейтс видимо не будет предпринимать решительных действий по созданию единой глобальной ОС, но техническая подготовка к этому шагу должна завершится в самое ближайшее время. Ещё одним реальным сдерживающим фактом является наличие пока ещё у очень многих Интернет провайдеров UNIX подобных операционных систем. Это не позволяет Билу Гейтсу задействовать в полной мере недокументированные части Microsoft TCP/IP, так как эти действие незамедлительно будут обнаружены UNIX с его полностью документированной сетевой протокольной системой. Однако есть данные, что Windows NT всё же постепенно вытесняет UNIX из мира Интернет. Похоже если мировое сообщество не предпримет реальных шагов по ограничению монопольной деятельности Microsoft нас ждут интересные события.