Краткое введение в основы защиты от вредоносных программ

Иван Галинский

A problem has been detected and Windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c

Si vis pacem, para bellum
Мира хочешь - к войне готовься

В наше время информация является одним из самых ценных ресурсов в мире и всегда найдутся те, кто этот ресурс захотят получить незаконным путём. Поэтому информационная безопасность — один из самых острых вопросов 21 века. Но, чтобы защищаться, нужно знать приёмы противника.

Изначально различные данные (в основном документы) хранили на бумаге. Это было достаточно надёжно, так как к наиболее важным документам доступ имел лишь ограниченный круг людей. Но на этом преимущества и заканчивались. Время шло, документов становилось всё больше, находить их становилось всё сложнее, что отнимало огромное количество времени. Тогда все записи стали сортировать, каталогизировать, что позволяло быстрее находить нужное, но однажды количество записей стало настолько большим, что и этот способ перестал эффективно работать. Люди стали искать решения. Были созданы вычислительные машины — но первые их образцы считывали информацию с перфокарт и возвращали её на те же перфокарты или непосредственно передавали другим машинам, например, различного рода станкам. Это и неудивительно, ведь первые компьютеры использовались в основном для автоматизации производственных процессов. Настоящая революция произошла, когда были созданы первые персональные компьютеры. И хотя они в то время стоили огромные деньги, популярность их росла с каждым годом. Такие ЭВМ предполагали более тесное взаимодействие с пользователем, и были сравнительно просты в использовании. Пожалуй, первым массовым персональным компьютером стал Apple II, имеющий интерфейс командной строки, что было в то время большим прогрессом, обладающий возможностью отображать цветную графику при (относительно) высоких разрешениях и способность воспроизведения звука. Стоил он относительно небольших денег, поэтому крупные и средние компании могли позволить себе иметь достаточно большое количество компьютеров для ускорения и упрощения бумажной работы.

Но прогресс не стоял. Компьютеры стали объединять в сети. Сначала сети были небольшими, в пределах одного филиала, затем масштаб повысился до компаний. А потом и сами сети стали объединять. Это происходило параллельно с разработкой сети для военных нужд. - ARPANET. Несмотря на то, что изначально ARPANET был создан для вооружённых сил США, он начал активно использоваться сначала в научной, а затем и в других областях. Появилось название «Интернет». Из дорогой бесполезной игрушки он постепенно (в геометрической прогрессии) превратился в незаменимый инструмент работы и развлечений для миллионов людей. Именно тогда любая информация стала потенциально доступной любому человеку.

В интернете большинство данных хранится на серверах — специально выделенных компьютерах для обработки запросов от клиентов, но ПО, используемое на серверах не идеально (как и везде), потому и стали возможными различные хакерские атаки. В то же время на обычных домашних компьютерах такая же ситуация, только из-за недостаточной защиты стали возможны автоматические атаки— вирусные.

Строго говоря, термин «вирусные атаки» не совсем правильный. Вирусы — это лишь отдельная ветвь вредоносных программ. Ведь существуют ещё и трояны, черви, шпионские модули (spyware). Всё вредоносное ПО на английском называется «malware», поэтому дальше будем использовать именно этот термин. Но прежде чем говорить о способах проникновения malware, необходимо кратко описать его виды.

Троянские кони (трояны) по классификации — вид вредоносных программ, проникающих в компьютер под видом полезных программ. В основном используют невнимательность пользователя.

Вирусы — разновидность программ, способных к размножению и распространению самих себя. Чаще всего вирусы переносятся через различные носители информации — например, дискеты или flash-диски. Вирусами они названы из-за того, что внедряют свой код в другие программы.

Черви — вредоносное ПО, способное размножаться и переноситься с одного компьютера на другой совсем без участия пользователя. Чаще всего распространяются через компьютерные сети, включая Интернет. В отличие от вирусов, они являются самостоятельными программами.

Руткиты (rootkit)— особый вид программ, цель которых является сокрытие следов присутствия злоумышленника или malware в системе.

Spyware — вид вредоносного ПО, перехватывающий конфиденциальные данные и определённым способом отправляющий их злоумышленнику.

Классификация — это конечно хорошо. Но это всего лишь теория. На деле же всё намного сложнее. Виды malware настолько сильно переплетены, что иногда возникают сомнения с определением класса очередного «творения».

К примеру, возьмём сильно нашумевшего червя **Rustock.C**. По способу проникновения — это червь, но он заражает системные файлы, являясь и файловым вирусом, тщательно маскирует своё присутствие в системе — руткит, да ещё и рассылает спам. Этот червь был создан в 2006 году. На данный момент его обнаруживает лишь один антивирус — Dr.Web.

Стоит отметить, что такая стойкость этого червя — результат многих приёмов. Один из самых главных — червь сам себя шифрует ключом, основанным на оборудовании компьютера, что не позволяет запускать его на других компьютерах. И ещё около полдюжины этих «трюков» обуславливают то, что он находился «на свободе» в течении 1,5 лет — абсолютный мировой рекорд! Итого имеем следующий набор — червь+спамбот(рассылка спама)+руткит+вирус. Это нагляднее всего показывает текущую ситуацию в мире malware.

Так как же проникает различного рода вредоносное ПО в компьютерные системы? Самый главный способ — уязвимости в приложениях. **Уязвимости — это ошибки в программировании** определённой программы (или даже прошивки устройства). Но не такие ошибки, которые просто приводят к зависанию или аварийному закрытию. Уязвимости — это **ошибки, позволяющие использовать себя для выполнения несанкционированных действий на целевой системе**. Чтобы лучше понять, как это происходит, рассмотрим пример на небезызвестном Adobe Photoshop CS2. В 2008 году в нём была обнаружена уязвимость в обработке BMP файлов. Чтобы напомнить, BMP файлы содержат точечные изображения. Значит, злоумышленник (далее — хакер) может создать такой BMP файл, который содержит не изображение, а последовательность машинных инструкций, выполняющих определённые действия. Вот так вот! Такие уязвимости называются **локальными уязвимостями**, так как они осуществляются только локально на одном компьютере, даже без сети.

Но как тогда проникают в компьютер черви, распространяющиеся через Интернет? Ответ: через **удалённые уязвимости**. Чтобы лучше понять, как они работают, рассмотрим пример: в интернет-браузере обнаружена та же ошибка, что и в Photoshop. Но есть один момент — чтобы открыть файл в Photoshop, пользователю нужно совершить определённые действия, но браузер ведь (в большинстве случаев) автоматически отображает картинки! Тогда пользователь, просто зайдя на заражённый сайт со специально сформированным BMP изображением, попадёт под атаку, сам того не подозревая! Казалось бы, что можно избегать сомнительных сайтов, обезопасив себя от рисков. Но были случаи, когда достаточно крупные сайты взламывались и на них устанавливались такого рода **эксплоиты**. Эксплоит — это программа, файл, или иной объект, использующий определённую уязвимость в своих целях, поэтому далее будем использовать данный термин.

Так что же может произойти со среднестатистическим пользователем? Он может в течении очень долгого времени пользоваться вполне честным сайтом, но в один прекрасный день этот сайт взломают, после чего сотни или даже тысячи пользователей окажутся под ударом.

Стоит отметить, что в принципе пользователь может даже и не заходить не на какой сайт, даже не пользоваться компьютером. Компьютер будет просто находиться в Интернете, например, закачивая какой-нибудь особо большой файл. А если в программе мгновенного обмена сообщений, например Skype (имел уязвимость, но она уже исправлена), обнаружат уязвимость **переполнения буфера**? Что же произойдёт? Для этого нужно понять, что такое переполнение буфера, и как оно работает.

В почти любой программе есть переменные (или их массивы). И каждая переменная имеет максимальное значение. А что произойдёт, если превысить это значение? Тогда переменная «выйдет из берегов», начав затирать собой машинный код, идущий перед ней. Обычно, если это происходит, программа выдаёт ошибку и закрывается. А теперь вопрос — раз переменная способна затереть собой машинный код, то можно ли вместо случайного значения подставить в переменную специально сформированный код (на самом деле всё намного сложнее, но принцип примерно таков)? Ответ: можно! В таком случае программа, оказавшаяся под ударом, послушно выполнит подставной код, после чего скорее всего закроется (но не обязательно).

А теперь вернёмся к делу — допустим, в Skype обнаружена именно такая ошибка, причём в обработке мгновенных сообщений. Злоумышленник просто посылает жертве специально сформированное сообщение, после чего происходит переполнение буфера и программа выполняет машинные инструкции, находящиеся в этом сообщении. Таким, образом, можно заставить компьютер скачать образец malware, например, вирус или шпионский модуль, а затем запустить его.

Проблема переполнения буфера настолько серьёзна, что ведущие производители процессоров внедрили защиту непосредственно в свои процессоры. Тогда, если происходит переполнение, программа просто закроется, не выполнив злонамеренного кода. В Windows нужно для этого включить в Панели инструментов, опции «Система» функцию DEP (Data Execution Prevention) для всех приложений. И, несмотря на то, что в Windows XP это реализовано не лучшим образом (в Vista лучше), многие атаки при этом отражаются.

Теперь мы знаем в общих чертах главные принципы заражения компьютерных систем. Возникает вопрос: так как же защитить себя от вредоносного ПО? Для этого рассмотрим главные методы борьбы, используемые в настоящее время, их преимущества и недостатки.

Антивирусы

Пожалуй, самое популярное и известное средство защиты на сегодняшний день. Изначально использовались для лечения файлов, заражённых вирусами, но сейчас детектируют также трояны, руткиты, шпионские модули и прочее. Современный антивирус — это сложный программный комплекс, обнаруживающий вирусы различными способами. Рассмотрим некоторые из них:

1. Самый первый способ — поиск по антивирусным базам. Если антивирус обнаруживает совпадение фрагмента с определённой записью в базе, выдаётся тревога. Однако, вирусы сегодня очень часто изменяются (мутируют) при размножении, что затрудняет их обнаружение этим способом.

2. Но malware имеет одну общую черту - странное поведение. Антивирус также может определять характер программы по её поведению. Например, если программа сразу после запуска начинает жадно лезть в системные папки, обращаясь к исполняемым файлам, антивирус может предупредить пользователя об этом, а уже пользователь решит, разрешать ей это или нет. Эта функция также встроена в некоторые файрволлы.
3. Эвристическое сканирование. Учитывая что, новые образцы malware появляются каждый день, нужна защита от них. Но как защититься от того, чего нет ни в одной антивирусной базе? Для этого нужно понять, что обычно делают вирусы, трояны и т.д. Ну, во-первых, чаще всего исполняемый файл малвари имеет небольшой размер, в пределах 200 кб. Второе — такие исполняемые файлы имеют в себе пути к различным критическим файлам (к примеру, «C:\WINDOWS\system32»), а также различные критические операции, которые присутствуют в-основном во вредоносном ПО. Критериев, конечно, намного больше, но в-целом эвристический анализ работает именно так. Но не всё так хорошо. Во-первых, эвристическое сканирование очень часто даёт ложные тревоги (особенно это касается различных crack или keygen программ), во-вторых занимает много системных ресурсов. В-третьих, хорошо сделанный образец malware эвристическое сканирование не найдёт.

Это самые главные возможности антивирусов. К сожалению, все они могут быть обмануты. Червь rustock.c трижды шифровал сам себя, скрывал своё присутствие в системе, каждый раз мутировал. И всё это успешно обходило и обходит антивирусные системы (и будет обходить).

Файрволлы

Имеют второе место по популярности среди средств защиты. Файрволл — программный или аппаратный комплекс, необходимый для фильтрации пакетов. Проще говоря, файрволл фильтрует сетевую активность. Например, компьютер хочет подключиться к очень злому сайту www.infected-site.com. Если в файрволле прописано правило, запрещающее подключения к этому сайту, то подключение не сработает. Но сейчас файрволлы (для Windows) — это не только фильтр пакетов, но ещё и разграничитель доступа, иногда и фильтр рекламы (напр. Outpost Firewall), ещё и сканер spyware, а иногда они поставляются с антивирусом (как в случае с Kaspersky Internet Security). Рассмотрим главные функции современных файрволлов.

1. Как и следует из спецификации, файрволл может разрешать и запрещать отправку данных по сети. Например, мы имеем программу обмена сообщений ICQ. Она должна подключаться только к серверу icq. Прописав это правило в файрволле, мы запретим любые другие подключения, чем повысим безопасность. И так поступаем с каждой программой.
2. Во многих файрволлах есть возможность контроля за действиями программы, то есть определять потенциально опасные действия и спрашивать пользователя, казнить или помиловать. Да, это та же функция, что и в антивирусах. Например, программа пытается внедрить себя в память другой программы. Файрволл при этом начнёт выдавать предупреждения. Правда, чтобы эффективно использовать этот метод, нужно быть внимательным к тому, что за программа пытается получить доступ.

И, как и в случае с антивирусами, эта защита может быть обманута. Главный враг файрволла — руткит, скрывающий следы присутствия malware в системе. И да, червь rustock.c это делает!

Собственно говоря, на большинстве компьютеров установлены только файрволл и антивирус. Поэтому, многие компьютеры остаются потенциально уязвимыми.

Так как же защищаться?

Как защищаться? Ну а как проникает всякая гадость в систему (в большинстве случаев)? Через уязвимости! Значит, чтобы избежать проникновения, нужно уязвимости устранять. А уязвимости — это ошибки. А ошибки можно исправить. Вывод один — **нужно регулярно обновлять ПО**! Во всех современных операционных системах есть функция автоматического обновления. Для Windows это можно контролировать через «Панель управления». Несмотря на обилие ошибок в продуктах Microsoft, исправления к ним выпускаются очень оперативно. Необходимо лишь их устанавливать вовремя, пока не стало слишком поздно. Но это не всё, ведь через «Автоматическое обновления» распространяются заплатки только для Windows, и нескольких близких к ней программ. А что если у нас есть уязвимый Photoshop CS2? Нужно идти на сайт производителя (в данном случае Adobe) и скачивать заплатку вручную. И так для всех сторонних программ. Но во многих программах

есть собственный модуль автоматического обновления (Firefox, к примеру), что заметно упрощает задачу. Необходимо отметить, что нужно не только использовать заплатки, но и использовать более безопасное ПО. К примеру, можно отказаться от Internet Explorer в пользу Mozilla Firefox или Opera. Пожалуй, самой радикальной (и часто эффективной) мерой является смена всей ОС на более безопасную. Но это тема для отдельного разговора.

Обновление для безопасности незаменимо. Но ведь существуют уязвимости, о которых не знает 99% хакеров. Но оставшийся 1% вполне может написать вирус, или ещё чего. Значит, одних лишь обновлений недостаточно. Вот сейчас и настало время ввести новое понятие — **пользователь**. Нет, это не тот пользователь, который находится в 50 см от монитора. Пользователь в данном случае — лишь учётная запись в системе. Каждый пользователь в системе имеет определённые **права**, то есть список тех действий, которые он может выполнять. В Windows по-умолчанию есть пользователь «Администратор», имеющий безграничные права. Вот в этом то вся и загвоздка. Большинство пользователей в Windows работают под администраторской учётной записью. Что это значит? Это означает, что любая программа, запущенная под администраторский записью, будет иметь безграничные права! Значит, чтобы не допустить «несчастных случаев», нужно завести ограниченную учётную запись, что легко делается через «Панель управления». Такая учётная запись не может изменять системные файлы, а также некоторые другие важные структуры. Для неё будет выделена своя папка «Мои документы», с которой и будет разрешено работать. У некоторых людей это обстоятельство вызывает «клаустрофобию». Но никто не запрещает открыть себе доступ к другим папкам. Для этого нужно войти систему под администраторской записью и выставить нужные права на папки. Здесь есть один очень важный нюанс — **файловая система для использования разграничения доступа должна быть NTFS**. Иначе эффекта не будет никакого! Если файловая система FAT32, то её можно легко преобразовать в NTFS стандартными средствами Windows, и эта процедура подробно описана в «Справке».

Теперь, когда у нас настроена ограниченная учётная запись, что же произойдёт при запуске вируса, или другой вредоносной программы? Она запустится, но полноценно «осесть» в системе не сможет! Ведь доступа к системным файлам у неё нет. Единственное, доступ к файлам, принадлежащим этому пользователю, она иметь будет. Но malware всё реже занимается вандализмом, но чаще старается получить контроль над системой. Разграничение доступа — один из самых эффективных способом борьбы с вредоносным ПО.

Глубже...

Все перечисленные выше методы — это лишь главные приёмы, используемые для защиты, и они доступны всем пользователям. Теперь пришло время применить более изощрённые приёмы, повышающие безопасность в разы. Но сначала нужно привести небольшое введение:

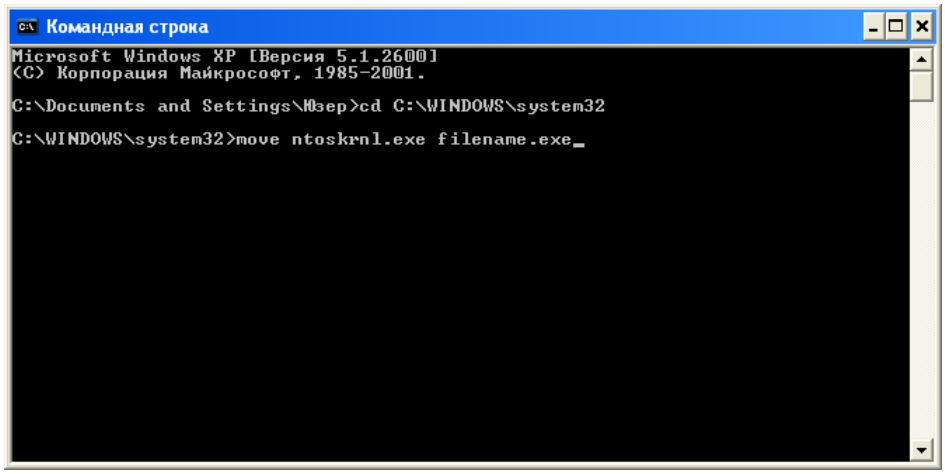
Качественного malware очень мало! Это раньше вирусописатели были по-настоящему талантливыми людьми, находящими уязвимости вручную и знающими компьютер от самых низких аппаратных уровней. Сейчас же большинство из них — так называемые «пионеры» - пишут такие «поделия», которые распознаются не по тому, что компьютер начал делать что-то, что вы и не думали делать, а по простой нестабильности! Помните — если компьютер начал не с того ни с сего зависать, выпадать в «голубые экраны», причём вы не устанавливали никаких программ или драйверов, то скорее всего это просто плохо написанный вирус, троян или ещё чего.

В таких случаях первое что можно сделать — это запустить «Поиск» через меню «Пуск» и начать искать файлы с расширениями .exe и .dll , созданные с того момента, как компьютер стал себя вести нестабильно. Пожалуй, это самый простой способ ручного обнаружения malware. Найдя что-то напоминающее образец вредоносного ПО (обычно у таких файлов малый размер), нужно зайти в Google (или любой другой поисковик), ввести в строку поиска название файла и просмотреть результаты. Если окажется, что это вирус, то можно посмотреть как с ним бороться там же, в результатах поиска. Если дельных советов не нашлось, то можно скачать программу-сканер наподобие Dr.Web CureIt!, которая просканирует (и возможно, вылечит) заражённые файлы.

Но следует рассмотреть и «меры предупреждения заболеваний». Ведь лучше избежать заражения, чем потом рвать на себе волосы из-за потерянных данных. Начнём с самого простого.

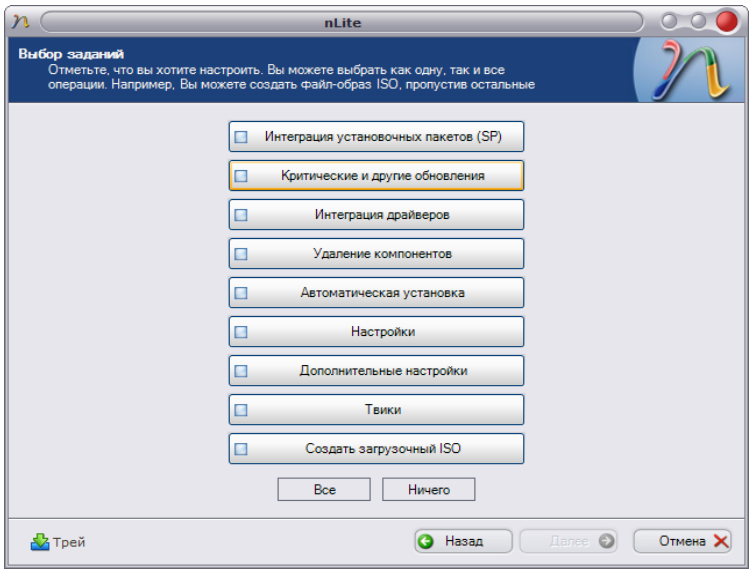
1. Систему лучше устанавливать на раздел диска, отличный от C:. Почему? А вот почему — многие вирусы просто напрямую обращаются к C:\WINDOWS ну и тому подобное. А что если у нас система установлена на диске D, а не на диске C? Тогда злая программа, обратившись к диску C в поисках «злачных мест» ничего не найдёт, впадёт в некоторое замешательство (может даже зависнет), но с системой ничего поделать не сможет. Ничего! Правда, образцы посерьёзнее так легко не обманываются, но на этот случай у нас есть ещё один приём.

2. Что делают вредоносные программы (в основном руткиты), когда получают доступ к системе? Они хотят в ней обосноваться, а для этого сразу лезут в файл *ntoskrnl.exe*. Этот файл — один из важнейших во всей операционной системе, так как является главным файлом ядра. Ядро — это самая главная часть операционной системе, ведь именно ядро «общается» с аппаратной частью компьютера, позволяя работать всем остальным программам. В нём содержится огромное количество данных, которые необходимы для работы вредного ПО. Поэтому мы сейчас сделаем «подставу». Перезагружаем компьютер, и перед тем, как появится эмблема Windows (до загрузки системы) начинаем нажимать кнопку F8. Теперь в появившемся списке выбираем «Безопасный режим с поддержкой командной строки». После некоторого времени появится окно командной строки, в котором сначала введём команду «*cd C:\WINDOWS\system32*» без кавычек (буква диска может варьироваться). Затем вводим «*move ntoskrnl.exe filename.exe*», где *filename.exe* — это новое имя для файла ядра, может быть любым, но латинскими буквами, без пробелов и не длиннее 8 символов (не считая приставки .exe). Затем вводим команду «notepad C:\boot.ini», и когда откроется Блокнот, к концу строки вида «*multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft (ну и так далее)*» мы добавим «*/kernel=filename.exe*» без кавычек, где *filename.exe* — это новое имя для ядра, которое вы выбрали. Осталось только перезагрузить компьютер. Для этого нужно нажать *Ctrl+Alt+Delete*, и в появившемся окне выбрать пункт «Завершение работы», а затем «Перезагрузка». Вот и всё! Теперь у нас есть ещё одна «линия обороны». **Но здесь есть один весьма и весьма неприятный нюанс.** Обновления Windows также просто напрямую обращаются к файлу ntoskrnl.exe, а мы ему поменяли имя! Ладно, тогда первое, что мы сделаем, это выставим опцию «скачивать обновления, пользователь определит время установки» в «Панели управления», компонент «Автоматическое обновление». Это необходимо, ведь система, начав автоматически устанавливать обновления, таких дров наколет, что систему придётся переустанавливать! Теперь, когда будет накапливаться достаточное количество обновлений, мы будем переименовывать файл ivanko.exe (или то, что у вас) обратно в ntoskrnl.exe (в Безопасном режиме с поддержкой командной строки введём «cd C:\WINDOWS\system32», затем «*move filename.exe ntoskrnl.exe*», потом «*notepad C:\boot.ini*», и в Блокноте стереть



«*/kernel=filename.exe*», а потом перезагрузиться, после чего устанавливать обновления, а затем делать обратное. Да, это трудоёмко! Но зато эффект в разы себя окупит — большинство вирусов и прочей гадости будут просто промахиваться, как пьяный мимо стула, ничего не успевая сделать. А сам процесс можно автоматизировать: для этого посмотрите статьи по созданию BAT файлов.

3. Так, заплатки мы устанавливать научились. А вдруг придётся переустанавливать Windows? Заново их качать? Подвергаться риску? Нет уж! Нужно их интегрировать прямо в установочный диск! Шаг первый: скачиваем Windows Updates Downloader с этой страницы: http://www.windowsupdatesdownloader.com/ProgramFiles.aspx и устанавливаем его. Далее переходим на эту страницу: http://www.windowsupdatesdownloader.com/UpdateLists.aspx , на которой сначала выбираем язык вашей системы, а затем скачиваем так называемый Update List для вашей версии системы. Например, у меня Windows XP SP2 на русском языке, значит на этой странице сначала выбираем язык «Russian», а затем скачиваем соответствующий Update List. Далее двойным щелчком по скачанному списку (или непосредственно через программу) открываем его. Вот и всё! Осталось только выбрать подходящую папку для закачек и отметить нужные нам обновления (по умолчанию отмечены все). Теперь нужно набраться терпения и дождаться завершения закачек. Когда скачивание завершится, мы будем иметь папку (которую указали прежде) с заботливо отсортированными обновлениями. Вот теперь самое время интегрировать их в дистрибутив. Первым делом создаём папку на диске, которую назовём, например *windows_cd*. Теперь вставляем загрузочный диск с Windows, и копируем все файлы с него (за исключением всяких дополнительных программ, обычно прилагающихся к пиратским копиям). Для этого просто заходим на диск и выделяем всё, кроме того, что ненужно. Теперь копируем всё это в нашу папку windows_cd. Этот шаг готов. А вот теперь наступает самое интересное. Сначала скачиваем программу nLite с этой страницы http://www.nliteos.com/download.html (или, если у вас Windows Vista, скачиваем vLite с этой страницы http://www.vlite.net/download.html). Теперь устанавливаем программу. Следует отметить, что эта программа не только интегрирует обновления, но ещё предоставляет возможность изменить некоторые настройки ещё «в зародышевом состоянии» системы, да и обеспечить установку без необходимости следить за ней, просто указав настройки по умолчанию. Но сильно этим увлекаться не советую, так как чтобы впоследствии изменить эти самые настройки, придётся потратить на это время, которого не всегда много. Запустив nLite, первым делом мы укажем путь к папке *windows_cd*, которую до этого создали. Затем мы укажем действия, которые мы хотим с этими дисками сделать. Обязательно отметьте опцию «Создать загрузочный ISO»!

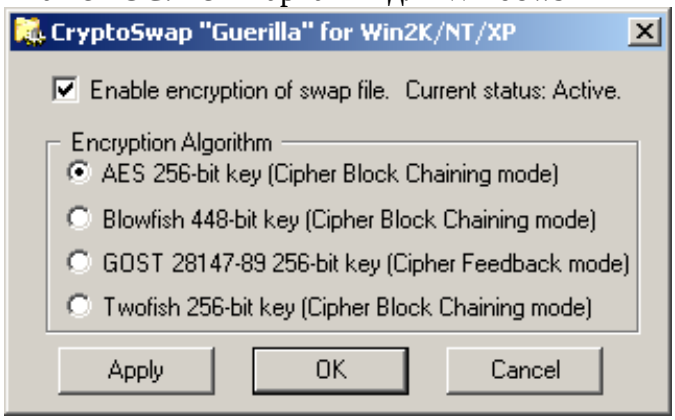


Таким образом, после интеграции всех обновлений, мы получим ISO файл, который затем легко записать на CD почти любой программой для записи дисков. В этом же окне nLite мы укажем опцию «Критические обновления» и, при необходимости, «Установочные пакеты». Интерфейс программы предельно понятен и переведён на русский язык. Тем не менее, если у вас есть сомнения по поводу использования,

посетите руководство на русском здесь: http://oszone.net/display.php?id=3757 Вот, теперь у нас есть диск с интегрированными обновлениями, и теперь не нужно будет каждый раз при переустановке системы скачивать их заново.

4. А теперь гипотетически предположим, что у нас есть абсолютно безопасная система. Она неуязвима? Нет! Мы забыли про самое главное в компьютере — его аппаратная часть. Да, в процессорах бывают ошибки! Причём это вовсе не секрет, например в процессорах серии Intel Core 2 есть ошибки, которые могут приводить к весьма неприятным последствиям. Что тут можно сделать? Нам — почти ничего. Можно устанавливать обновления для BIOS (Basic Input Output System), но вовсе не гарантировано то, что они исправят эти ошибки. Кроме того, перепрошивка BIOS — процесс весьма рискованный и может привести к нерабочей системе, и придётся нести материнскую плату в сервисный центр. Но на данный момент не известно о существовании malware, которое бы пользовалось этими ошибками. Значит, единственное что здесь можно сделать — это расслабиться и не беспокоиться.

5. Что делает система, когда ей не хватает оперативной памяти? На этот случай во всех современных ОС есть так называемый «файл подкачки», также называемый «swap-файлом» или «виртуальной памятью», расположенный на жёстком диске. На некоторых системах (в частности, различных клонах UNIX, например Linux) может быть и специально отведённый под эту задачу раздел диска. Только в отличие от UNIX, использующего файл подкачки только тогда, когда оперативная память «забита под завязку», Windows использует виртуальную память всё время. Допустим, у нас есть программа prog.exe, которая запущена, но никто ей не пользуется. Тогда система просто перемещает её в файл подкачки, дабы она не занимала места в оперативной памяти. Плюс данного подхода очевиден: оперативная память (которой много не бывает), очищена от неиспользуемого кода. Но отсюда же выходят и минусы: во-первых, скорость чтения жёсткого в лучшем случае равна 150 Мб/сек, в то время как скорость чтения к оперативной памяти составляет несколько гигабайт в секунду. Но с этим ещё можно смириться. Есть недостаток куда похуже: **в файл подкачки зачастую попадают весьма конфиденциальные данные**, доступ к которым, в-принципе, получить легче, чем к «настоящей» оперативной памяти. Причём swap файл (по умолчанию) не очищается при выключении компьютера, то есть в нём могут оставаться данные ещё предыдущей сессии. К счастью, есть решения для этой проблемы. Самое простое — это просто избавиться от файла подкачки и забыть его, как страшный сон. Но это подойдёт только тем, у кого есть достаточное количество оперативной памяти. А если нет? Тогда выходит другое решение, куда элегантнее предыдущего. Это **шифровка виртуальной памяти.** Для этого есть уже готовые решения, как коммерческие, так и бесплатные. Рассмотрим одну из лучших бесплатных реализаций. Это CryptoSwap. Изначально эта программа предназначалась для Linux систем, но впоследствии была перенесена на Windows. Скачать её можно с этой страницы: http://www.geocities.com/phosphor2013/list.htm Затем на этой странице нужно выбрать версию программы для вашей ОС. Есть варианты для Windows 2000/NT/XP и для Windows 9x/Me. Про совместимость с Vista ничего не известно, поэтому рисковать не советую. Далее скачиваем архив, распаковываем его и запускаем файл *CryptoSwap.....exe*. В архиве это единственный исполняемый файл. Далее следуем указаниям установщика (ничего особенного), после чего перезагружаем компьютер. Всё! Теперь у нас swap



файл шифруется случайным ключом при каждой загрузке системы, а при выключении он очищается. Если вы чувствуете, что время выключения системы сильно увеличилось, можно отключить функцию очистки файла подкачки. Для этого заходим в папку установки программы (обычно это C:\Program files\CryptoSwap) и запускаем файл «*disableswapwipe.reg*», не забыв согласиться на появившееся диалоговое окно. Если вы хотите изменить настройки шифрования или вовсе отключить его, запустите окно управления программы (для этого обычно достаточно щёлкнуть по соответствующему ярлыку на Рабочем столе), после чего подкорректировать желаемые функции.

6. Как работает большинство червей? А как выглядит обычный (настоящий, ленточный) червь? Маленькая хитрая головка с присосками и хвост длиной метров в 3. Как бы иронично это не было, именно так и работают компьютерные черви. Сначала через ошибку переполнения буфера (или другую уязвимость) на компьютере появляется голова (ведь просто через уязвимости много не сделаешь), которая и закачивает «хвост», содержащий полезную нагрузку. Иногда бывает по-другому (в новых червях) — сначала закачивается «голова», которая закачивает дропер (от слова drop — бросать), который в свою очередь не только скачивает основное тело, но и шифрует его определённым ключом. По такому алгоритму работает Rustock.C. Но современные черви — это почти автономные зонды-роботы для отправки на Марс, главная цель которых — выжить (и размножиться). Например, активно используется функция контроля популяции (обычно с централизованным управлением). Ведь, если червь будет чуть ли не на каждом компьютере в Интернете, его быстро обнаружат и обезвредят. А это вирусописателям не надо, ведь при помощи malware сегодня выполняют вполне коммерческие цели, вроде рассылки спама и сбора данных о пользователях (spyware может быть встроено в червя). Во-вторых, сам программист должен писать максимально правильный код, который (ни в коем случае) не должен вызывать зависания, «синие экраны», повышенную системную нагрузку, в-общем всё то, что могло бы выдать малварь с головой. А некоторые черви могут подгружаться в память антивируса или файрволла! Такая импровизированная «атака с тыла» получается. Думаю, о последствиях говорить не стоит. Ведь антивирус имеет практически безграничный контроль над системой! Конечно, есть способы защиты от подгрузки вредоносного кода, но они специфичны для каждой системы (слишком много факторов). Черви сегодня не создают новых сетевых подключений (подсаживаются на уже существующие), не создают новых процессов в памяти (подгружаются в уже существующие), некоторые даже не создают новых файлов (работают в оперативной памяти, после перезагрузки не выживают). Обнаружить и обезвредить ещё неизвестного науке экземпляра очень трудно, но возможно, причём вручную. Для этого нужно знать анатомию операционной системы, архитектуру компьютера, многие скрытые нюансы и иметь немного сноровки. Тогда даже самый серьёзный вирус будет обнаружен. Главное — просто захотеть.

Важные мелочи

Ну и напоследок можно представить несколько простых правил, которые, тем не менее, могут сыграть весьма важную роль.

1. Не следует усложнять. Правило KISS (Keep It Simple, Stupid) действует всегда. Чем меньше программ установлено в системе (особенно работающих в фоновом режиме или как сервисы), тем система безопаснее. Например, IM-клиент Miranda (или QIP Infium) позволяет обмениваться сообщениями сразу по нескольким протоколам, при этом обладает простотой и не требователен к системным ресурсам. Это ведь лучше, чем постоянно пользоваться полудюжиной различных программ, не так ли?

2. Всегда стоит использовать последние версии программ (а особенно — драйверов). Таким образом избегается куча проблем с ошибками, нестабильностью, и т.п. Но под «последними версиями» я имею ввиду «последними *стабильными* версиями». Не надо скачивать ещё не отлаженные alpha или beta версии.

3. Как можно строже указывайте правила в файрволле. Тем самым можно уменьшить риск несанкционированной отправки данных.

4. Windows хранит свои настройки в так называемом Реестре. Там же находится и большое количество настроек, доступа к которым через «Панель управления» обычно не получить. Но ручное изменение настроек реестра — занятие долгое и нудное, поэтому можно воспользоваться программой XP Tweaker. Она предоставляет достаточно удобный интерфейс для управления наиболее популярными опциями в реестре. Скачать можно здесь: http://xptweak.sourceforge.net/download.htm После распаковки и установки программа предложит создать точку восстановления, что я рекомендую сделать. Всё, теперь продукт готов к употреблению! Опций очень много, поэтому рекомендую прочитать официальную справку здесь: http://xptweak.sourceforge.net/help/ Дальше действуйте по предпочтениям (и нуждам).

5. Когда будете устанавливать права доступа к папкам и файлам, не переусердствуйте! Если разрешить себе доступ ко всей и вся, все плюсы разграничения доступа вдруг станут минусами.

6. Ну и напоследок, будьте внимательны! Не запускайте подозрительные файлы, не лазите по всяким «очень интересным» сайтам (ну а если очень надо, подумайте о замене Internet Explorer на Opera или Firefox, если ещё не сделали этого). От невнимательности не меньше бед, чем от ошибок в программировании (они, кстати, тоже возникают из-за невнимательности).

Заключение

Интернет будут всегда. Крупные эпидемии — явление вполне закономерное, как кризисы в капиталистических странах, обновляющие и очищающие. Избежать их не получится. Рано или поздно что-то и к нам проникнет, но можно этот момент оттянуть, главное не отставать от прогресса. *Periculum in mora* (Опасность в промедлении)