Dr.WEB®
Антивирус

Защити созданное

Анализ активных заражений и лечение инфицированных систем с помощью антивирусного ПО компании «Доктор Веб»

Учебный курс

Оглавление

Введение

Данный курс посвящен проблеме обнаружения и устранения различных угроз. Он предназначен, в первую очередь, для сотрудников отдела технической поддержки компании ООО «Доктор Веб», но будет также полезен всем, кто хочет научиться с помощью продуктов Dr.Web лечить ПК от вирусов и устранять все последствия активности вредоносного ПО.

В пособии приведена классификация вредоносных программ по типам, дан перечень суффиксов и префиксов, которые используются в обозначении названий вирусов компанией «Доктор Веб». Также выделены основные признаки инфицирования компьютера и описаны пути проникновения вирусов на него.

Основная же часть посвящена непосредственно борьбе с вредоносным ПО и восстановлению системы, для чего мы подробно рассмотрим средства и способы поиска вредоносных программ. В работе будет использоваться пакет Антивирус Dr.Web, лечащая утилита Dr.Web CureIt! и Shark-режим сканера Dr.Web.

1. Немного истории

Так сложилось, что многие пособия по какой-либо теме начинают с краткого экскурса в историю вопроса. Мы не будем делать исключение, и в этом вводном разделе ознакомимся с историей компьютерных вирусов и ступенями развития Антивируса Dr.Web как наиболее оптимального средства для борьбы с вредоносным ПО.

1.1. Вирусы: от задумки до эпидемии

Впервые термин «компьютерный вирус» был озвучен в 1983 году американским ученым Фредом Коэном и определен им как «программа, которая может "инфицировать" другую программу, внедряя в нее свою копию». Но приложения, подходящие под это описание (способные самостоятельно размножаться), существовали и ранее. Первым вирусом считается игра Pervading Animal, появившаяся в 1960 году, которая хоть и создавалась не с целью кому-то навредить, но выполняла базовую функцию вируса — умела размножаться. Однако это была не заслуга ее автора, а чистая случайность — копии, заполняющие весь жесткий диск, создавались из-за ошибки в программном коде, а не по умыслу создателя.

Идею самовоспроизводящихся программ изложил «отец» компьютера Джон фон Нейман еще в 1949 году, но тогда его слова мало кто воспринял.

Но заинтересованные нашлись, хоть и спустя долгое время — в 1975 году появился вирус The Creeper, который не причинял вреда, лишь выводил сообщение на экран. Но он уже умел самостоятельно распространяться по сети, став первым сетевым вирусом в истории. Он же породил и первый антивирус — программу Reeper, являющуюся по сути таким же сетевым вирусом — Reeper распространялась по сетям, никак себя не проявляя, а если ей удавалось найти на компьютере The Creeper — она его стирала.

Первой эпидемией компьютерных вирусов можно считать произошедшую в 1986 году эпидемию достаточно безвредного вируса Brain, который за год своего существования поразил множество компьютеров по всему миру, хотя изначально создавался для определения уровня компьютерного пиратства в Пакистане.

В 1990-х годах существенно расширился ассортимент вредоносных программ и спектр совершаемых ими действий, а в нашем веке не способна подхватить вирус разве что микроволновая печь — КПК и мобильные телефоны, долгое время считавшиеся неуязвимыми, ныне часто подвергаются заражению. Что же касается компьютерных систем, в 2000-х годах защищенных систем не осталось: Mac OS X, вирусов для которой не существовало, перестала быть абсолютно безопасной — 16 февраля 2006 года был официально подтвержден факт обнаружения первого вируса для этой операционной системы (для сравнения, первый вирус для IBM PC появился в 70-е годы). А вредоносные программы уже нескольких вариаций существуют даже для FreeBSD (например, FreeBSD.BackDoor.IRC.1).

1.2. Dr.Web: от исполняемого файла к антивирусному комплексу

Началом истории антивируса Dr.Web можно считать 1992 год, когда Игорем Даниловым была создана первая версия антивирусной системы Spider's Web (прототип Dr.Web), одним из компонентов которой был сканер, носящий название Doctor Web. В сканере впервые была реализована идея «прокрутки» кода программ в эмуляторе процессора для поиска неизвестных вирусов. Антивирус Spider's Web получил достаточно широкую известность, и в 1994 году начались продажи сканера, переименованного в Dr.Web.

В 1996 году Dr.Web, на тот момент версии 3.06b, впервые был представлен на сравнительном тестировании полиморфных вирусов, проводимом журналом Virus Bulletin. Результаты, показанные антивирусом, оказались более чем впечатляющими как по уровню противодействия

полиморфным вирусам, так и по возможностям эвристического анализатора. В статье журнала Virus Bulletin о программе Dr.Web (версия 3.08) был особо отмечен эвристический анализатор антивируса, который в режиме Параноик определил 100% полиморфных вирусов.

1999 год можно считать годом рождения резидентного антивирусного модуля SpIDer Guard, который мог всегда находиться в оперативной памяти ПК и проверять на лету все открываемые и изменяемые файлы. Стоит отметить, что прототип резидентного сторожа, программа Spider, входил еще в комплект Spider's Web, но в продажу он тогда не поступал.

Продолжая работать в направлении антивирусной защиты почтового трафика, разработчики Dr.Web в 2002 году создали первый в мире почтовый антивирус — SpIDer Mail, являющийся компонентом антивирусного пакета Dr.Web.

2003 стал годом рождения компании ООО «Доктор Веб», которой отныне и выпускались все программы с товарным знаком Dr.Web®.

В 2004 году появилась первая версия корпоративного антивируса — Dr.Web Enterprise Suite, позволявшего осуществлять централизованную защиту большого количества рабочих станций на предприятиях. Тогда же началось бета-тестирование нового компонента Dr.Web — дополнительной вирусной базы, детектирующей шпионское и рекламное ПО.

В 2005 году выходит лечащая утилита drweb-cureit.exe, позднее названная Dr.Web CureIt!, которая могла проверять и чистить компьютеры от вирусов без установки, при работающем резидентном антивирусе другого производителя.

2007 год ознаменовался выходом решения Dr.Web Антивирус + Антиспам и новой версии антивируса 4.44 с полной поддержкой операционной системы Windows Vista и антируткитом Dr.Web Shield.

2008 год был богат на достижения. В Москве открылся новый современный офис «Доктор Веб», стартовал проект «Есть покрытие» — Антивирус Dr.Web, предоставляемый как услуга от интернет-провайдера, оказался весьма удобным и быстро приобрел популярность. А 28 октября впервые был представлен компакт диск Dr.Web LiveCD для экстренного лечения и восстановления критически поврежденных систем.

В 2009 году дан старт стипендиальной программе для студентов, работающих в области ИТ и защиты информации. Тогда же компания «Доктор Веб» представила первый в России антивирус для Mac OC X и сетевой аналог Dr.Web CureIt! — лечащую утилиту Dr.Web CureNet! А в составе Dr.Web Security Space Pro появился долгожданный брандмауэр.

2010 год прошел под эгидой борьбы с небывалой эпидемией Trojan.Winlock (*http://vms.drweb.com/virus/?i=18308*). На сайте «Доктор Веб» открылся раздел бесплатной помощи всем пострадавшим от подобных вирусов. Для облегчения восстановления критически поврежденных систем создается пакет Dr.Web LiveUSB, аналог Dr.Web LiveCD. Также проходят релизы версий антивируса, призванных защитить мобильные устройства под управлением Android, Symbian OS и Windows Mobile.

Если вы хотите подробнее узнать историю Антивируса Dr.Web, посетите страницу: *http://company.drweb.com/history*, а вехи развития проекта Dr.Web CureIt! можно прочитать здесь: *http://www.freedrweb.com/cureit/history*.

2. Признаки заражения

Признаков, что на компьютере функционирует какая-либо вредоносная программа, может быть много, и здесь мы рассмотрим основные. Но стоит отметить, что само наличие признаков заражения — уже большая удача, поскольку, заподозрив неладное, можно начать экстренную проверку ПК на вирусы и внеочередную архивацию важных данных. Гораздо хуже, когда вредоносная программа вообще никак себя не проявляет, ибо в этом случае пользователь не подозревает о ее существовании вплоть до момента ее срабатывания, а порой так и остается в неведении. В такой ситуации владелец ПК не знает о том, что его персональные данные уже похищены, а персональные счета обналичены злоумышленниками.

К счастью, идеально скрыть деятельность программы очень трудно и, так или иначе, догадаться о наличии вредоносного ПО в системе можно. Ниже перечислены признаки заражения компьютера, сгруппированные по области их проявления.

2.1. Со стороны операционной системы

1. Компьютер часто зависает.
2. ОС загружается медленнее, чем раньше.
3. Заметно снижается быстродействие ПК, приложения работают медленнее, игры «притормаживают».
4. Периодически возникают критические системные ошибки (BSOD).
5. Изменяется внешний вид окон и системных сообщений.
6. Возникают разнообразные сообщения, внешне схожие с системными, но содержащие шутки или бессмысленные наборы символов.
7. В центре экрана появляются баннеры рекламного или порнографического содержания, которые нельзя убрать. Зачастую баннер загораживает всю рабочую область монитора.
8. Операционная система перестает загружаться.
9. Невозможно загрузить Windows в безопасном режиме.
10. Невозможно открыть диск или какую-либо папку.
11. Изменились настройки рабочего стола, и вернуть их в прежнее состояние вручную не удается. Например, изменилось разрешение или цветовая гамма.
12. Появились неизвестные значки в области уведомлений.
13. Невозможно создать точку восстановления системы или архивировать данные с помощью встроенных средств резервного копирования.
14. Перестают запускаться системные утилиты, или выдается сообщение о нехватке прав для их запуска.

2.2. Со стороны аппаратной части и периферии

1. Компьютер внезапно перезагружается, хотя скачков напряжения и команд на перезагрузку не было.
2. Встроенный динамик или колонки компьютера воспроизводят мелодии или странные звуки.
3. DVD-привод открывается и закрывается без запроса пользователя.
4. Клавиши на клавиатуре перестают соответствовать обычно производимым им действиям. Например, клавиша Пробел функционирует как Esc.
5. Индикатор жесткого диска горит, даже когда вы не выполняете на ПК никаких действий.
6. Резко сокращается количество свободного места на дисках.
7. Резко сокращается объем доступной оперативной памяти.
8. Принтер стал недоступным, или невозможно напечатать документы.

2.3. Со стороны почты и Интернета

1. Проявляется сетевая активность, инициируемая процессами или приложениями, которые вы не запускали.
2. Брандмауэр сообщает о попытке проявить сетевую активность приложениями, которые вы не устанавливали.
3. Часто обрывается связь или существенно замедляется работа интернет-соединений.
4. Электронные письма возвращаются с сообщением о невозможности доставки их адресату (обычно в строке Отправитель там значится Mailer-Daemon или Mail Delivery System, это может быть связано с блокированием инфицированного сообщения почтовыми серверами).

2.4. Со стороны браузера

1. Перестают открываться все или некоторые интернет-сайты (как правило, первыми блокируются сайты обновления Windows и ресурсы по информационной безопасности).
2. Изменяются настройки браузера (зачастую обнуляются опции безопасности и подменяется домашняя страница).
3. В окне браузера появляются посторонние элементы.

2.5. Со стороны приложений

1. Папки или файлы изменяются без участия пользователя.
2. Перестает обновляться антивирус.
3. Отключаются или начинают работать с ошибками антивирус или брандмауэр.
4. Без участия пользователя запускаются или закрываются приложения.
5. В списке активных процессов появляются неизвестные процессы с непонятными названиями.

Если вы обнаружили что-либо из вышеперечисленного на своем ПК, это еще не гарантия, что компьютер инфицирован, поскольку проблемы могут быть вызваны множеством других факторов. В этом случае необходимо действовать в двух направлениях:

- Установить антивирус, если это не было сделано ранее, для уже имеющегося — скачать последние обновления. После этого выполнить полную проверку компьютера на вирусы.
- Исправить ошибки в установленном ПО и системные сбои — «замусоренный» реестр может быть виновником очень большого числа проблем. Проверьте работоспособность тех узлов, которые вызывают сбои, скачайте последние версии всех используемых программ, установите все обновления для своей версии Windows.
- Проверить работоспособность аппаратной части ПК — неисправность модулей оперативной памяти, жесткого диска и других компонентов может непредсказуемо влиять на поведение системы.

3. Основные сведения о вредоносном ПО

3.1. Пути проникновения вредоносного ПО на компьютер

Обычно под термином «зараженный компьютер» понимают ПК, на котором есть один или несколько вредоносных объектов. На самом деле заражены всего несколько файлов, а с остальной «здоровой» частью в принципе можно продолжать спокойно работать.

Итак, представим, что ваш компьютер кристально чист, то есть его жесткие диски не содержат ничего, кроме установленной еще до покупки операционной системы. Но как только вы начинаете устанавливать скачанные из Интернета программы, записывать музыку, фильмы, работать с дисками, открываются каналы для доступа вредоносного ПО на ваш компьютер. Ниже перечислены пути, используемые вирусами для проникновения на ПК.

Система автозапуска. Достаточно просто сделать так, чтобы при вставке флеш-карты в компьютер автоматически запускалась определенная программа. Автозапуск есть практически на всех компакт-дисках, а все версии Windows, начиная с XP, сами начинают анализировать содержимое флешки или диска, чтобы запустить подходящую программу для работы с ними. Если все в порядке, то системный автозапуск выдаст вам окошко с выбором вариантов дальнейших действий. Если же на сменном носителе содержится вирус, то есть вероятность, что первым попадет в оперативную память именно он (при отсутствии на ПК резидентного антивируса или при отсутствии в его базе соответствующих сигнатур). Этот путь проникновения — один из самых распространенных на сегодняшний день.

Локальная сеть. Если ваш компьютер подключен к какой-либо локальной сети, то невнимательность отдельных пользователей может поставить под угрозу безопасность всех ПК в сети, став источником распространения вредоносного ПО. Компьютерные черви очень легко распространяются по локальным сетям, где политика безопасности достаточно мягкая, и пользователи имеют много прав и разрешений по доступу на другие компьютеры сети. Кроме этого, размножению вирусов способствуют и ошибки в Windows, еще не устраненные Microsoft. Стоит отметить, что именно стремительное распространение вирусов по локальным сетям чаще всего становилось причиной глобальных вирусных эпидемий. Одной из последних можно считать эпидемию вируса Win32.HLLW.Shadow.based (подробнее: *http://news.drweb.com/show/?i=204&c=5&lng=ru&p=27*), который использовал уязвимости в ОС Windows.

Интернет. Многие сайты, независимо от содержимого, могут быть инфицированы вирусами или вредоносными скриптами. Пиратские дистрибутивы программ тоже с высокой долей вероятности могут быть носителями вирусов или троянцев. Конечно, поймать вирус можно и на чьем-либо официальном сайте (от огрехов никто не застрахован, и специалисты по безопасности тоже люди, и тоже ошибаются), но шанс заразиться намного выше именно на ресурсах с «халявой» или порно. Сюда же можно отнести инфицированные сообщения электронной почты — многие крупные эпидемии развивались именно посредством обмена пораженными письмами.

Уязвимости в установленном ПО. По данным исследований, проведенных специалистами по информационной безопасности, ПК, на котором работают программы с известными уязвимостями, при отсутствии защитных систем может быть заражен в течение 3–5 минут.

Сам пользователь. Очень часто невнимательность и излишняя доверчивость могут привести к тому, что вы сами установите на компьютер все необходимое злоумышленнику вредоносное ПО. Этот метод распространения вирусов (и метод интернет-мошенничества) называется *социальная инженерия* — хакер лично общается с пользователем, и с помощью разнообразных уловок добивается, чтобы жертва установила на свой компьютер какую-либо программу, открыла файл, посетила сайт и т. д. Если вы будете осмотрительны и не слишком доверчивы, то эта угроза не столь опасна.

3.2. Какие объекты могут подвергнуться заражению?

Многие пользователи, когда-либо серьезно пострадавшие от вредоносного ПО, начинают излишне бояться вирусов и с опаской относиться буквально ко всем получаемым данным. С одной стороны, эти опасения не беспочвенны, но когда речь идет о работе с файлами, можно точно сказать, какие из них могут быть инфицированы, а какие нет.

Итак, какие же именно файлы могут содержать в себе вирусный код?

Исполняемые файлы программ. Любой файл, который, будучи запущенным, получает возможность частичного контроля над компьютером, может быть опасен — внедренный в него вирусный код при запуске также получит возможность действовать. Это все файлы с расширениями .exe, .com, .bat, .msi, .lnk, .cmd, .scr. Также возможна ситуация, когда вредоносный исполняемый файл маскируется под файл другого типа с помощью ложного расширения. Отображение расширений может быть отключено в настройках системы, и в таком случае открывая, как можно судить по пиктограмме, avi или jpg файл, вы запускаете троянца или шпионскую программу. Иногда можно встретить даже файлы, имеющие такое имя: "Имя_файла.jpg.exe".

Загрузочные сектора носителей информации. Это нельзя назвать файлами, но стоит помнить, что вирус может быть и там.

Приложения, написанные на Flash. Небольшие игры и программы, имеющие расширение .swf, также могут быть заражены.

Файлы скриптов и скрипты на веб-страницах. Файлы с расширением .js или .vbs — это скрипты на языке Java или Visual Basic. Обычно они используются на веб-страницах, к примеру, для регистрации пользователей или при входе их на определенный сайт под своей учетной записью. Но эти же скрипты могут содержать и вирусный код, который, получив доступ к браузеру, может существенно помешать работе, установив на рабочий стол или прямо в браузер баннер, отключить который невозможно. В принципе, эти файлы тоже можно отнести к исполняемым, но без специальной программы работать они не смогут.

Документы MS Office. Документы, созданные в программах этого пакета, — основное и единственное место обитания макровирусов. Этот пункт можно считать несущественным, поскольку отключение макросов в документе (Word и Excel сразу выдают запрос на запрет или разрешение макросов) многократно снижает вероятность активации вируса и дальнейшего заражения. Стоит отметить, что в среде MS Office 2007 и новее вирусов замечено не было, но если вы используете более старые версии, следует соблюдать осторожность.

Документы PDF. Используя уязвимости программного обеспечения Adobe, некоторые вирусы способны встраивать себя в pdf-документы и при их открытии инфицировать ПК. Чаще всего такие вирусы блокируют сетевой экран и загружают из Интернета «основной» вирус, который и поражает систему и распространяется по сети. Уже несколько лет эти вирусы имеют широкое распространение, во многом за счет того, что файлы данного формата являются основой обмена документами в Интернете.

Медиафайлы. Существует несколько видов троянцев, способных поражать аудио- и видеофайлы. Этот вид угроз не получил большого распространения, но опасными могут быть уязвимости в медиапрогрывателях, которые встречаются часто и могут быть использованы злоумышленниками.

Все остальные объекты на компьютере можно считать относительно безопасными — txt-файлы, архивы, если в них нет исполняемых файлов, изображения и файлы данных различных программ, и т. д.

3.3. Папки размещения вредоносных файлов

Попадая на компьютер, вирусу необходимо в первую очередь куда-либо сохранить свои файлы, откуда он потом будет запускаться и действовать. Чаще всего вирусы размещают себя в следующих местах:

- В корневых папках дисков, чаще всего — C:\
- В профиле пользователей ПК (C:\Documents and Settings\ в Windows XP и C:\Users\ в Windows Vista и Windows 7)
- Во временных папках (C:\Windows\Temp, C:\Documents and Settings\Temp, C:\Users\Temp)
- В папке операционной системы (как правило, C:\WINDOWS\) и вложенных в нее папках (чаще C:\WINDOWS\system\, C:\WINDOWS\system32\, C:\WINDOWS\system32\drivers\, C:\WINDOWS\Temp).

4. Настройка ПК и приложений для обеспечения защиты от вирусов и интернет-угроз

Одной из важнейших (если не самой важной!) составляющих компьютерной безопасности является не качество установленного антивируса и даже не сам факт его наличия в системе, а банальная осведомленность и аккуратность пользователя. Известно, что любой человеческий вирус легче предупредить профилактическими мерами, нежели лечить уже проявившуюся после инкубационного периода заразу. То же самое можно сказать о компьютерных вирусах — если пользователь не соблюдает правила компьютерной «гигиены», то рано или поздно он попадет с ситуацию, где антивирус окажется бессилен. Ниже приведен перечень основных действий пользователя, выполнение которых обеспечивает системе достаточно высокий уровень вирусной безопасности (разумеется, эти методы не исключают установку антивируса).

4.1. Настройка Windows

Достоверно известно, что наибольший урон и глобальные эпидемии были вызваны сетевыми червями, которые эксплуатировали те или иные уязвимости в Windows. По сей день продукт от Microsoft остается наиболее распространенной ОС, используемой в офисах и на домашних ПК. Ниже мы рассмотрим ряд действий, позволяющих если не устранить, то существенно минимизировать возможности вирусных атак, использующих системные ошибки.

1. ***Работа с ограниченными правами пользователя.*** Чаще всего домашний или офисный ПК имеет единственного системного пользователя, имеющего права администратора. В то же время стоит помнить, что все программы, запускаемые пользователем, имеют тот же максимум прав, что и он сам. Таким образом, работая с правами администратора, вы открываете вирусам многие двери.

   Чтобы избежать многих проблем, достаточно создать на компьютере учетную запись с ограниченными правами и использовать при работе именно ее, переключаясь на пользователя *Администратор* (проще всего так и назвать полноправную запись) только для установки новых программ или внесения изменений в системные настройки.

   Чтобы создать новую учетную запись, нажмите *Пуск –> Панель управления –> Учетные записи пользователей*. Выберите *Создание учетной записи*, в открывшемся окне введите имя для этой записи (например, *Работник*) и нажмите *Далее*. В следующем окне отметьте флажком *Ограниченная запись* и выберите *Создать учетную запись*. Теперь при загрузке Windows на экране будет появляться меню выбора пользователя.

   Постоянно работая с ограниченной записью, вы существенно сократите возможности вирусов по поражению вашей системы и размножению в ней.

   Примечание. Существует учетная запись с именем *Гость*, с помощью которой можно зайти в Windows, не имея собственной учетной записи. Удалить эту запись нельзя, но ее необходимо *Отключить*.

   Использование UAC. В среде Windows Vista и Windows 7 по умолчанию включен UAC (User Account Control — Контроль учетных записей), который требует подтверждения на выполнение любых значительных действий в системе. Желая избавиться от постоянных запросов, пользователи отключают UAC, но с точки зрения безопасности делать это **категорически не рекомендуется!** Подробнее об этой функции можно прочитать, например, здесь: *http://www.java.com/ru/download/faq/uac.xml*.

2. ***Регулярное обновление Windows.*** Постоянно поддерживая ОС в актуальном состоянии, вы избежите атак, осуществляемых через известные уязвимости. **Самый простой вариант для реализации этого пункта — включить *Автоматическое обновление*.** К сожалению, большая часть используемых у нас в стране копий Windows — пиратские и, следовательно, не могут обновляться автоматически. В такой ситуации можно устанавливать обновления, вручную скачав их с сайта компании Microsoft. Но наилучшим решением будет приобрести

лицензионную копию Windows, что позволит не только получать все обновления автоматически, но и даст круглосуточный доступ к службе технической поддержки.

Для проверки наличия еще не установленных обновлений можно использовать утилиту Microsoft Baseline Security Analyzer, скачать которую можно по ссылке: *http://technet.microsoft.com/en-us/security/cc184924*.

3. ***Отключение наиболее уязвимых компонентов системы.*** Такие компоненты, как *Удаленный помощник, Удаленный реестр* и им подобные, рекомендуется отключать, если вы их не используете. Для отключения воспользуйтесь руководством из раздела 5.
4. ***Использование программ сторонних разработчиков.*** В состав Windows входит множество компонентов, альтернативой которым являются продукты (в том числе бесплатные) сторонних разработчиков. Для обеспечения максимальной безопасности рекомендуется использовать следующее ПО сторонних производителей.
   - *Брандмауэр.* Брандмауэр является частью системы безопасности Windows, поэтому уязвимости в нем ищутся злоумышленниками в первую очередь. Чтобы обезопасить себя, установите брандмауэр другой фирмы или используйте комплексный антивирусный пакет (например, пакеты от Dr.Web: Dr.Web Security Space Pro или Антивирус Dr.Web Pro).
   - *Браузер.* Поскольку с его помощью пользователь работает в Интернете, браузер и ошибки в нем представляют наибольший интерес для хакеров. Использование бесплатных браузеров (например, Opera, Chrome или Firefox) значительно повышает уровень безопасности при работе в сети. Также можно использовать защитные плагины, например Noscript или ADBlock Plus для Firefox.
   - *Почтовый клиент.* Встроенный в Windows клиент Outlook Express и компонент пакета Microsoft Office Outlook являются первыми мишенями взломщиков, специализирующихся на различных почтовых диверсиях. Использование сторонних программ (например, Thunderbird или The Bat!) значительно снижает риск подвергнуться атаке через почтовый клиент.

При желании заменить можно даже пакет Microsoft Office, например его бесплатным аналогом OpenOffice, который поддерживает все типы документов, созданных в MS Office.

Сама необходимость перехода на стороннее ПО вызвана тем, что широко распространенные продукты Microsoft имеют значительное количество уязвимостей, активно использующихся хакерами. Применяя для работы менее распространенные программы, вы существенно снизите риск пострадать от эксплойта в них.

5. ***Отключение автозапуска со съемных носителей.*** Существует целый ряд вирусов, загружающихся в память ПК при установке в привод инфицированного диска или флеш-накопителя. Чтобы предотвратить активацию таких вирусов, необходимо запретить автозапуск со всех съемных носителей. В Windows версий Vista и 7 отключить автозапуск можно через соответствующее меню, а в Windows XP для этого необходимо внести ряд корректив в настройки групповой политики:

   Нажмите *Пуск –> Выполнить, в строке введите gpedit.msc –> OK*. В открывшемся окне выберите *Политика Локальный компьютер –> Административные шаблоны –> Система –> Отключить автозапуск*. В диалоговом окне отметьте флажком пункт *Включен*, в выпадающем списке укажите *Всех дисководах* и нажмите *Применить*, затем *OK*.

Примечание. Многие антивирусные пакеты, например Антивирус Dr.Web, позволяют запретить автозапуск со съемных носителей.

Внимание! К съемным носителям относятся не только флеш-карты и лазерные диски, но и вообще *любые устройства, имеющие накопитель и использующие USB (или любой другой порт, например eSATA) для подключения к ПК*! То есть можно передать вирус с одного компьютера на другой даже через фотоаппарат или mp3-плеер. Съемные жесткие диски, хоть и не считаются системой сменными носителями, представляют не меньшую угрозу, и в плане безопасности к ним требуется предельное внимание.

4.2. Настройка установленного ПО

Поддерживать установленное на компьютере программное обеспечение в актуальном состоянии не менее важно, чем обновлять ОС. Теоретически абсолютно любую ошибку в программе можно использовать для причинения вреда системе в целом. Будет это кратковременный сбой или серьезная порча данных – не важно, но возможность причинения ущерба есть. Чтобы этого избежать, важно следить за состоянием имеющегося ПО и своевременно скачивать обновления или новые версии.

Многие программы автоматически проверяют наличие обновления через Интернет. Отсюда вытекает простое правило: **не следует отключать в настройках программ автоматическое обновление или, если его нет, уведомление о новых версиях**.

Но многие программы не следят за собственной актуальностью, и в таком случае необходимо проявить активность пользователю. Например, воспользуйтесь утилитой Secunia Personal Software Inspector от компании Secuna. Скачать последнюю версию утилиты можно по адресу: *http://secunia.com/vulnerability_scanning/personal*. После инсталляции утилита сканирует установленное ПО, после чего просматривает сайты соответствующих производителей и при необходимости позволяет в автоматическом режиме обновлять все установленные приложения.

Также стоит учесть, что количество вредоносного ПО, использующего уязвимости в продуктах Adobe, стабильно увеличивается. Чтобы противостоять этим угрозам, можно действовать по двум вариантам:

- В настройках Adobe Reader отключить запуск объектов JavaScript (по умолчанию эта опция включена). Это не гарантия безопасности, но большая часть уязвимостей используется злоумышленниками с помощью скриптов.
- Использовать альтернативные программы просмотра PDF-файлов (например, бесплатное приложение FoxIt Reader – *http://www.foxitsoftware.com/downloads*).

Внимание! Ни один программный продукт не требует столь частой актуализации, как антивирус. Новые вирусы пишутся постоянно, и вирусные базы обновляются с очень высокой частотой. Например, антивирус от компании «Доктор Веб» по умолчанию автоматически обновляется каждые полчаса!

В то же время компьютер с антивирусом, базы которого последний раз обновлялись больше недели назад, можно считать абсолютно незащищенным. Поэтому старайтесь обновлять антивирус как можно чаще и **ни в коем случае не отключайте автоматическое обновление!**

4.3. Настройка браузера

Поскольку описать тонкости настройки всех существующих браузеров в рамках нашего курса просто невозможно, здесь мы укажем ключевые параметры, от которых зависит защищенность браузера от вирусов и интернет-атак. Необходимо:

- **Блокировать незапрашиваемые всплывающие окна.** Это нужно не только для избавления от части рекламы на сайтах, но и чтобы не допустить проникновения вредоносного ПО на жесткий диск.
- **Не сохранять пароли.** Первое интернет-правило – ваш ПК не должен знать ваших паролей к интернет-ресурсам. В противном случае, при удачной атаке или вирусном заражении, все пароли попадут к хакеру. И если среди них будут почтовые или банковские данные – вы можете потерять многое.
- **Ограничить применение JavaScript.** Эта опция есть не во всех браузерах, но при ее наличии можно включить применение JavaScript, запретив ВСЕ дополнительные опции этого раздела (например, разрешение на изменение размеров окна, строки состояния и т. д.).
- **Включить антифишинговый фильтр.**

- **Блокировать невидимые окна (отключить IFrame).** Невидимые окна могут использоваться злоумышленниками для скрытого перенаправления пользователей на инфицированные сайты. Как отключить IFrame в различных браузерах, описывается в разделе 5.
- **При работе с pdf-файлами сохранять их на диск, не открывая в браузере.** Учитывая широкое распространение угроз для pdf-формата, безопаснее сохранять файлы этого типа на жесткий диск и открывать только после проверки антивирусом.

Как задать эти опции в вашем браузере, вы можете уточнить в его справочной системе.

4.4. Общие правила безопасности при работе с Интернетом и почтой

Поскольку большая часть вредоносного ПО распространяется через Интернет и, в частности, электронную почту, то особенно важно знать правила, позволяющие снизить риск заражения вирусом именно через эти источники:

1. **Внимательно относиться к любым сообщениям, полученным от неизвестных людей.** Это относится как к сообщениям в IM-системах, так и к электронным письмам. В сообщении может содержаться не просто спам (к которому все уже привыкли), но и какие-либо вредоносные скрипты или ссылки. В идеале, неизвестные сообщения не стоит открывать вообще.
2. **Не переходить по ссылкам в сообщениях из непроверенных источников.** Где бы и какую бы ссылку вам ни предлагали, лучше ей не пользоваться. Вряд ли вы упустите что-то хорошее, зато точно не попадете на очередной фишинговый сайт или не скачаете вредоносный скрипт.
3. **Не открывать и не скачивать вложения из писем от неизвестных адресатов.** Если ссылка может вести на вредоносный сайт, то вложенный в письмо файл может сам оказаться троянцем, шпионом или вирусом. Вообще, переходить по ссылкам из писем можно только убедившись в подлинности адресата.
4. **Не скачивать программы с непроверенных сайтов.** Порталы с «халявным» ПО — любимое место обитания вирусописателей, вследствие чего большая часть свободно распространяемых через пиратские сайты программ инфицирована. Если вам потребовалось какое-либо приложение — загрузите его с официального сайта производителя — и честнее, и безопаснее.
5. **Избегать ресурсов порнографического содержания.** На сайтах с «клубничкой» всегда много посетителей, и мошенники стараются разместить вредоносное ПО именно там, чтобы украсть как можно больше частных данных или денег.
6. **Выбирать сложные пароли.** Чем длиннее и сложнее ваш пароль — тем труднее злоумышленнику будет его взломать. Руководствуясь этим, старайтесь придумывать пароли, имеющие максимальную длину и содержащие как можно больше различных символов (строчные и заглавные буквы, цифры, допустимые спецсимволы).
7. **Исключить повторение паролей.** Необходимо, чтобы для каждого сетевого ресурса (страница в соц. сети, электронная почта, Интернет кошелек и т. д.) у вас был отдельный пароль. Это не позволит злоумышленникам, взломавшим один из ваших аккаунтов, получить доступ к остальным.
8. **Не обращать внимания на мошеннические уловки.** Если вы получили электронное письмо или мгновенное сообщение, якобы от администрации сервиса, в котором требуется подтвердить, например, активность аккаунта и сообщить свои логин и пароль, не обращайте внимания — это мошенничество. **Никогда и никому не сообщайте свои учетные данные, даже если требование выглядит как официальный запрос от администрации ресурса (это обман)!**

9. **Не сообщать о себе в Интернете слишком много.** Интернет — зона активного общения, где каждый человек может рассказать о себе все, что сочтет нужным. Разумеется, какой-то минимум данных о себе указать необходимо, но активно делиться с интернет-сообществом подробностями своей жизни не рекомендуется — зная о вас достаточно много, злоумышленники смогут использовать эти сведения, чтобы скомпрометировать вас или попытаться действовать от вашего имени.
10. **Контрольные вопросы должны быть сложными.** Пароль ко многим сетевым сервисам (например, к почте) можно восстановить с помощью *Контрольного вопроса*. Например, вы забыли пароль от почтового ящика. Через соответствующую ссылку на сайте вы запрашиваете новый пароль. Система выводит вам вопрос, который вы сами указали при регистрации и ответ на который (в идеале) известен только вам. В случае правильного ответа вы сразу можете ввести новый пароль и продолжить пользоваться сервисом. При выборе контрольного вопроса постарайтесь сделать так, чтобы никто, даже из ваших близких, не смог подобрать верный ответ на него. Указывать в качестве пары "вопрос-ответ" какие-либо очевидные вещи (например: «Сколько ног у человека?» «Две») тоже недопустимо.

4.5. Противодействие атакам типа «социальная инженерия» с помощью подручных средств

Термин «социальная инженерия» объединяет в себе несколько видов интернет-угроз, общей чертой которых является тот факт, что внимательность жертвы играет решающую роль в успехе атаки. Уловок для пользователей может быть множество — фишинговые ссылки, ложные письма из банков или администрации каких-либо сетевых ресурсов и многое другое. Особенно стоит отметить, что различные виды социальной инженерии всегда направлены на одно и то же: получить личные данные пользователя, будь то пароли от веб-сервисов или конфиденциальная информация и банковские данные.

Чтобы справиться с мошенниками, использующими данный метод атаки, требуется не так много. Соблюдение простых правил из приведенного ниже списка помогает заметно снизить вероятность потери информации:

1. Если вы получили письмо с требованием сообщить или подтвердить ваш пароль от любого ресурса — удаляйте его, какие бы страшные угрозы в нем ни содержались (удаление аккаунта, обнуление счета и т. д.). **Администрации сетевых ресурсов, а уж тем более банки НИКОГДА не запрашивают у пользователя какие-либо данные.**
2. Если вы получили от своего знакомого письмо или сообщение странного содержания, например, похожее на спам или имеющее ссылки на какие-то ресурсы, — свяжитесь с респондентом любым другим способом (например, по телефону) и уточните, что и зачем он вам послал. Не исключено, что его аккаунт взломан и используется злоумышленниками.
3. Если какие-либо сторонние ресурсы предлагают перейти на страницу, где вам придется ввести свои данные (например, ссылка на сайт vkontakte.ru) — потратьте время, чтобы вручную ввести текст ссылки в окно браузера — это полностью исключит возможность попадания на фишинговый сайт (существует много методов маскировки истинных путей ссылок).
4. Прочитав в Интернете про «легкий» способ взломать какой-либо сайт, лучше не проверяйте описанный метод в действии. Хакеры никогда не афишируют, какие уязвимости им удалось найти, а сыграть на любопытстве пользователей, заставив тех сделать что-то нужное киберпреступникам, они могут.
5. Установите на ПК антивирусный пакет, содержащий веб-антивирус и антифишинг, — это намного обезопасит любые ваши действия в сети. Хорошим примером может служить пакет Dr.Web Security Spase Pro.

4.6. Резервное копирование важных данных

Большое количество резервных копий, хранящихся в разных местах, — надежная гарантия того, что ценная информация не пропадет. Сколь бы внимательны вы ни были, как бы ни был надежен используемый антивирус — всегда найдется причина краха, которую никто не учитывал. Это может быть пожар, прорванные трубы или банальное ограбление — в таких ситуациях любые защитные меры, кроме резервного копирования, будут бесполезны.

Оптимальным можно считать хранение информации в трех не связанных друг с другом местах. Например, на рабочем и домашнем компьютерах, и на съемном жестком диске. Флешки, ввиду своей «нежности» и частого «хождения по рукам» не могут считаться полноправным резервным хранилищем. Обратите внимание, что две копии в разных папках одного жесткого диска — это все равно одно хранилище — при повреждении диска погибнет, вполне вероятно, все содержимое.

Приступая к сохранению информации, нужно ответить на три вопроса:

- **Какая информация требует резервирования?** Сохранять имеет смысл только личные и рабочие данные — папки и документы, созданные или полученные пользователем. Базы данных, адресные книги, почтовые и фотоархивы — тоже необходимо внести в этот список. Сюда можно с некоторой натяжкой отнести собираемые в течение долгого времени музыкальные коллекции, если составлялись они по принципу «с миру по нитке». Что НЕ следует сохранять: кинофильмы, дистрибутивы программ, скачанные из Интернета музыкальные коллекции. Подобная оценка данных исходит из того, что скачать фильм или дистрибутив из Интернета — дело считанных минут, а восстановить семейные фотографии в случае утраты будет просто невозможно. Аналогичные примеры можно привести и с другими типами данных.
- **На каких носителях будет содержаться информация?** Оптимумом для хранения архивных копий можно считать жесткие диски, причем не обязательно съемные. Объясняется это просто: лазерные диски не способны гарантировать качественное длительное хранение (хоть производители и заверяют обратное), а флешки часто используются для переноса информации, и при небрежном использовании легко сгорают. Кроме этого, при невысокой цене жесткие диски имеют просто огромный объем, иногда позволяющий не задумываться над первым вопросом.
- **Где будет храниться информация?** Ответ на этот вопрос зависит от степени конфиденциальности данных. Например, те же семейные фотографии можно хранить дома, на работе и на съемном диске. Для архивирования же документооборота компании такой подход не применим — цена рабочих данных может быть слишком высокой, чтобы позволить им «уйти домой» к кому-либо из сотрудников, а уж о хранении их на переносном диске не может быть и речи. В таком случае имеет смысл хранить один жесткий диск с зашифрованными данными в сейфе. При уходе ответственного лица с работы жесткий диск снимается с компьютера и кладется в сейф, а ключ сдается на вахту. Утром ключ берется с вахты, открывается сейф, диск устанавливается в ПК, вводится пароль для доступа к зашифрованному содержимому, и можно начинать работу. Описанная процедура является стандартом работы с секретной информацией по требованиям ФСБ.
- **Сколько копий информации необходимо иметь?** Вы можете выбрать оптимальный вариант и приобрести один или два дополнительных носителя, понадеяться на авось, ограничившись двумя копиями, или проявить крайнюю осторожность и изготовить пять копий. Исходя из ответа на этот вопрос, можно будет рассчитать затраты средств на резервные накопители и времени на сам процесс архивации.

Продумав детали, можно приступать к копированию. С точки зрения экономии дискового пространства и сохранения структуры данных, имеет смысл использовать специальные программы-архиваторы (см. ссылки в Приложении 2). Со стороны безопасности лучше переносить данные чистым копированием — нет сжатия, нет единого архива, повреждение которого сведет на нет все усилия.

4.7. Настройка антивируса Dr.Web

Если на ваш компьютер уже установлен антивирус Dr.Web, нужно одновременно с настройкой ПК настроить и его. Общие настройки антивируса можно выполнить, нажав правой кнопкой мыши на значок Dr.Web в области уведомлений и выбрав пункт *Инструменты –> Настройки*. Конфигурацию каждого модуля антивируса можно произвести, выбрав соответствующий пункт меню антивируса, и в раскрывающемся списке нажав *Настройки* (Например: SpIDer Mail –> Настройки).

Общие настройки. Для обеспечения максимального уровня защиты, в разделе общих настроек перейдите на вкладку *Расширенные* и отметьте флажками все присутствующие здесь пункты. Для подтверждения внесенных изменений нажмите *Применить*, затем *ОК*.

Примечание. В режиме максимальной защиты, при установке некоторых обновлений Windows, флажок с пункта *Запрещать модификацию важных объектов Windows* потребуется временно убрать.

Настройки Родительского контроля. Функцию Родительского (офисного) контроля можно использовать для ограничения доступа пользователей к интернет-ресурсам определенного содержания (например: насилие, порнография и т. д.), а также полной блокировки доступа к сети и/или сменным накопителям. Также возможно запретить доступ пользователя в указанные папки на локальном ПК. Для этого потребуются соответствующие параметры Родительского контроля и пароль к нему. Опции настраиваются для каждого пользователя, и все изменения необходимо вносить, войдя в систему под соответствующим именем.

Внимание! В случае утери пароля от Родительского контроля его восстановление невозможно — потребуется полностью переустановить антивирус Dr.Web.

Примечание. Обо всех случаях ложного срабатывания модуля Родительского контроля или пропуске сайтов запрещенной тематики необходимо сообщать в компанию «Доктор Веб».

Прочие параметры антивируса перенастраивать, как правило, не требуется — опции, установленные по умолчанию, обеспечивают надежную защиту ПК. Полную информацию о настройке и использовании антивируса Dr.Web можно получить в «Руководстве пользователя» (*http://download.geo.drweb.com/pub/drweb/windows/doc/drweb-600-win-space-ru.pdf*).

5. Обнаружение вредоносного ПО

5.1. Начальные этапы вирусной активности

Чтобы начать активно действовать в системе, вирусу необходимо разместить себя на жестком диске (опционально) и в оперативной памяти (обязательно). По сути, существует три способа скрытого попадания вирусов в оперативную память:

- загрузка вируса одновременно с ОС при помощи различных методов автозапуска (о них далее);
- загрузка вредоносной части вируса из Интернета и/или «сборка» его в памяти заражаемого ПК;
- удаленный ручной запуск вируса на вашем ПК по сети (с помощью различных средств доступа).

5.1.1. Автозагрузка вирусов

Начнем с методов автоматической загрузки вирусов в оперативную память ПК. Способов загрузить какое-либо приложение одновременно с ОС существует достаточно много, и здесь мы постараемся разобрать их все:

Запуск с помощью реестра

Ниже приведены ветви, добавление в которые ключа может инициировать запуск указанной программы. Например, файл C:\file.exe будет загружаться автоматически при старте Windows или при входе пользователя в систему, если ключ

«FILE.EXE” со значением “C:\file.exe”

находится в одной или нескольких ветвях реестра, перечисленных ниже:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce]

В этих ключах важны параметры "run" и "load" (приложения, указанные в первом ключе, загружаются после входа пользователя в систему, вторые – до).
Особенно стоит обратить внимание на программы, которые могут попасть в автозагрузку через групповую политику, поскольку они зачастую не отображаются в программе MSConfig (о ней далее) и большинстве менеджеров автозагрузки. Проверьте ветвь:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run]

и при необходимости удалите оттуда все ключи.

Очень важное место, откуда могут запускаться программы, – это ветвь реестра Windows Logon:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
Она содержит достаточно много ключей, но нам будут нужны только некоторые:

Shell – ключ задает перечень файлов, которые запускаются вместе с Windows. По умолчанию значение ключа Shell: "Explorer.exe" для Windows 2000\XP и "taskman, progman, wowexec" для Windows 98\NT. Все посторонние файлы, перечисленные здесь, можно удалять – с высокой долей вероятности это файлы вирусов.

Userinit – ключ присутствует только в версиях Windows новее Windows 98 (за исключением NT). Он задает файлы, загружаемые при входе пользователя в систему. Значения по умолчанию: “userinit, nddeagnt.exe” для Windows NT и “ X:\WINDOWS\system32\userinit.exe,” для Windows 2000\XP, где X – раздел установки ОС. Все посторонние файлы, перечисленные здесь, нужно отправлять на анализ в вирусную лабораторию – с высокой долей вероятности это файлы вирусов.

System – аналогично предыдущему, этот ключ присутствует только в NT-версиях Windows (NT\XP). Он задает перечень файлов, запускаемых как системные в момент инициализации ОС. Значение по умолчанию: “lsass.exe, spoolss.exe” для Windows NT, и “lsass.exe” для Windows XP. В среде Windows 2000 параметр не обрабатывается.

VmApplet – ключ, присутствующий только в Windows 2000\XP, отвечает за активацию приложений, позволяющих пользователю корректировать системные параметры. Значение по умолчанию: «rundll32 shell32, Control_RunDLL «sysdm.cpl»».

Все описанные ключи определяют поведение процесса *winlogon.exe* в условиях его нормального функционирования. Если файл инфицирован или подменен вирусом с аналогичным функционалом, его поведение может резко отличаться от стандартного, но ключи реестра здесь уже ни при чем.

Порядок обработки этих ключей следующий: загрузившись, процесс winlogon.exe запускает файл "Userinit.exe", отвечающий за старт программной оболочки. Userinit исполняет сценарии регистрации, настраивает сетевые соединения и запускает процесс "Explorer.exe". Если в ключе Userinit прописаны и другие файлы – они также исполняются на этом этапе. Если старт процесса Userinit почему-либо невозможен, winlogon начинает обработку файлов, указанных в ключе "Shell".
Таким образом, возможно запустить приложения еще до входа пользователя в Windows, если в реестре вместо "Userinit.exe" прописан "userinit.bat" и существует соответствующий пакетный файл со списком программ, которые необходимо выполнить.

Запуск через назначенные задания

Все может быть очень просто – вирус не модифицирует ключи реестра, а просто добавляет в планировщик задание на загрузку себя в память после завершения загрузки Windows. Узнать, какие программы запускаются по расписанию, можно, посмотрев содержимое папки C:\Windows\Tasks.

Запуск через папку Автозагрузка

Добавить сюда ярлык еще проще, чем прописать новое задание. Проверить содержимое папок автозагрузки нужно по двум адресам:

- C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка – из этой папки запускаются программы, установленные для всех пользователей.
- C:\Documents and Settings\Имя_Пользователя\Главное меню\Программы\Автозагрузка – отсюда запускаются программы, установленные только для конкретного пользователя.

Важным фактором является то, что через ключи реестра можно сменить папку, которая будет обрабатываться ОС как источник ярлыков для автозагрузки. Проще говоря, абсолютно любую папку на компьютере можно задать в качестве папки автоматической загрузки. За это отвечают два ключа:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders] – ключ "Common Startup"="%ALLUSERSPROFILE%\Главное меню\Программы\Автозагрузка" – общая для всех пользователей папка автозагрузки. Изменив это значение, можем указать другую папку (например, C:\Кучавирусов).
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders] – ключ "Startup"="%USERPROFILE%\Главное меню\Программы\Автозагрузка" – автозагрузка для текущего пользователя.

Примечание. Обработку папки Автозагрузка можно отменить вручную. Для этого во время загрузки Windows необходимо зажать клавишу Shift.

Примечание. Вирусная активность по отношению к папке автозагрузки может проявляться также в подмене ярлыков. Например, в папке хранится ярлык для какой-либо установленной программы, но указывает он совершено не на тот файл, что значится в названии. Или же ярлык ссылается на командный файл, который запускает не только то, что значится в названии, но и исполняемый файл вируса или троянца.

5.1.2. Точки начальной вирусной активности

Тем или иным способом загрузившись в память ПК, вирус может сразу начать свою разрушительную деятельность, а может сначала позаботиться о собственной безопасности и доступе к нужным ему функциям ОС, которые обычно бывают защищены. Ниже перечислены точки, через которые вирус начинает действовать, уже будучи активированным и загруженным в память.

Ключи реестра

Разбор начальной вирусной активности мы начнем с реестра. Зачастую именно его ключи подвергаются модификациям, чтобы позволить вирусу обходить систему безопасности ПК или загружать вредоносный код при старте Windows. Для работы с реестром используется программа Regedit (*Пуск –> Выполнить –> regedit, OK*). Нас будут интересовать ключи и соответствующие им значения различных ветвей реестра следующего типа:
Ключи параметров безопасности. Они находятся в следующих ветках:

- \SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ (любой куст)
- \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ (любой куст)
- HKLM\SYSTEM\ControlSet00x\Services\SharedAccess\Parameters\FirewallPolicy\ (x – цифры 1–9)

К этой группе относятся ключи, задающие настройки безопасности интернет-соединений, групповых политик и параметры работы брандмауэра.
Ключи регистрации системных служб и драйверов:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Services (x – цифры 1–9)

Они управляют регистрацией и запуском системных служб и драйверов. Стоит отметить, что внесение в эти ключи вредоносных драйверов значительно затрудняет восстановление системы и очистку ее от вирусов, при этом значительно расширяя возможности самого вредоносного ПО.
Ключи настроек операционной системы и приложений. К ключам этой группы относятся очень многие ветви реестра, в частности все, что перечислены в этой книге. Они могут использоваться вредоносными программами двояко: чтобы нарушить работу ОС и приложений, либо чтобы украсть персональные данные пользователя из различных программ (особенно опасно здесь запоминание различных паролей браузером).

Сетевые компоненты Windows

Сюда относятся все элементы системы, которые отвечают за функционирование компьютера как одной из составляющих сети. Изначально все, описанное ниже, создавалось исключительно для обеспечения или оптимизации работы сети, но вирусы могут использовать многие из этих возможностей для своих целей. Чаще всего деятельность вредоносной программы проявляется одним из перечисленных ниже способов.

Открытые сетевые порты. Каждый компьютер имеет один физический провод, соединяющий его с Интернетом или локальной сетью. Но ведь этот провод используется всеми программами, требующие доступ к сети. Чтобы использовать единое соединение могли все приложения,

в протоколах TCP и UDP было введено понятие Сетевой порт – виртуальная точка подключения, которых может быть создано до 65535, и каждая из которых нумеруется от 0 до 65535. Соответственно, каждой программе выделяется один или несколько портов для взаимодействия с сетью. Контролем безопасности портов занимается брандмауэр.
Каждый сетевой порт характеризуется одним из состояний:

- SYN_SENT (соединение устанавливается)
- ESTABLISHED (соединение установлено)
- TIME_WAIT или CLOSE_WAIT (соединение закрывается)
- LISTENING (готов к приему соединений)

В то же время для многих программ, сканирующих порты (к ним относятся некоторые легальные, например, брандмауэр, и нелегальные – снифферы), любой порт может иметь состояние *Открыт*, *Закрыт* или *Скрыт*. *Открытый порт* готов принять подключение, *Закрытый* – нет, а *Скрытый порт* не виден из сети, поэтому его состояние определить невозможно. Основной интерес с точки зрения взломщика представляют именно *Скрытые порты*, поскольку атака на закрытые невозможна, а открытые контролируются брандмауэром.
Проверить состояние портов на ПК можно с помощью системной утилиты Netstat. Для работы с ней откройте *Командную строку* (*Пуск –> Все программы –> Стандартные –> Командная строка*), введите *netstat*, задайте необходимые параметры и нажмите клавишу *Enter*. Для просмотра допустимых параметров введите *netstat /?*.
Далее приведена ссылка на список портов, зарегистрированных за различными программами и службами. Зная, какое ПО установлено на компьютере пользователя, можно попытаться соединиться с его ПК, используя порты, которые открываются соответствующими программами и имеют статус LISTENING, то есть готовы к приему входящих соединений. Кроме этого, можно использовать какое-либо вредоносное ПО, чтобы создать несколько портов с состоянием LISTENING, что значительно облегчит взломщику соединение с компьютером жертвы. Полный список общеизвестных и зарегистрированных портов можно прочитать здесь: *http://ru.wikipedia.org/wiki/Список_портов_TCP_и_UDP*.
Встроенные утилиты удаленного администрирования. В Windows присутствует несколько инструментов, позволяющих удаленно управлять компьютером. Изначально эти программы создавались для облегчения взаимодействия пользователей, но их (вернее, ошибки в них) очень быстро освоили злоумышленники. Перечень компонентов, обеспечивающих непосредственный удаленный доступ, и которые необходимо отключить:

- ***Удаленный реестр.*** Отключение: выберите *Пуск –> Настройка –> Панель управления –> Администрирование –> Службы*. Найдите службу *Удаленный реестр* и, дважды нажав на нее левой кнопкой мыши, выберите *Тип запуска –> Отключено*.
- **Удаленный помощник.** Отключение: выберите *Пуск –> Выполнить –> gpedit.msc, OK*. В открывшейся консоли перейдите: *Политика "Локальный компьютер" –> Конфигурация компьютера –> Административные шаблоны –> Система –> Удаленный помощник*. В правом окне консоли для параметра *Запрошенная удаленная помощь* задайте *Отключен*, нажмите *Применить*, а затем *OK*. По умолчанию значение этого параметра *Не задано*, что на самом деле позволяет запускать удаленного помощника.
- **Удаленный рабочий стол.** Отключение: выберите *Пуск –> Выполнить –> gpedit.msc, OK*. В открывшейся консоли перейдите *Конфигурация компьютера –> Административные шаблоны –> Компоненты Windows –> Службы терминалов*. В правом окне консоли для параметра *Разрешать удаленное подключение с использованием служб терминалов* задайте *Отключен*, нажмите *Применить*, а затем *OK*.

Браузеры

В настоящее время браузер стал не просто средством просмотра html-страниц, а «всем и сразу», вплоть до игровой станции, за счет поддержки огромного количества скриптов, и медиастудии, что обусловлено поддержкой различных плагинов для работы с аудио и видеоинформацией.

Плагины и скрипты — самая уязвимая часть браузера, ибо применить их возможно не только на благо пользователя и для его удобства, но и ему же во вред. В частности, вредоносное ПО может использовать возможности вашего браузера поддерживать следующие элементы веб-страниц:

Скрипты. Это небольшие элементы кода, написанные на языке JavaScript ли VisualBasic. Вредоносные скрипты, как правило, скрыто загружают вирусы на ПК, занимаются непосредственной «сборкой» вредоносной программы на пораженном компьютере, или производят несанкционированное перенаправление на посторонние сайты (в основном инфицированные).

Невидимые окна (inline frame, сокращенно IFRAME). Iframe — это обычный html-тег, создающий невидимое окно, которое нельзя закрыть обычными способами. С его помощью отображается баннерная реклама, а если речь идет о вредоносном использовании тега — он позволяет переадресовывать пользователя на посторонний инфицированный сайт за счет скрипта, внесенного внутрь этого тега. Отключить обработку тега iframe в различных браузерах можно следующими способами:

- ***Opera (http://ru.opera.com).*** В главном меню нажмите *Инструменты –> Общие настройки*, в появившемся окне перейдите на вкладку *Расширенные* и в левой части выберите *Содержимое*. Затем нажмите *Настроить стили* и в открывшемся окне снимите флажок с пункта *Включить inline-фреймы*, после чего нажмите *OK*.
- ***Internet Explorer.*** В главном меню нажмите *Сервис –> Свойства обозревателя*, в открывшемся окне перейдите на вкладку *Безопасность* и, выбрав зону *Интернет*, нажмите кнопку *Другой*. Откроется окно параметров безопасности. В нем необходимо найти пункт *Запуск программ и файлов в окне IFRAME* и установить соответствующие ему флажок напротив *Отключить*. После нажатия *OK* необходимо перезапустить браузер, чтобы изменения вступили в силу.
- ***Firefox (http://www.mozilla.com/ru/firefox).*** В этом браузере для прекращения обработки IFRAME будет удобно использовать дополнение Noscript (*https://addons.mozilla.org/ru/firefox/addon/noscript*).

Элементы ActiveX. Если элементы управления ActiveX разрешены, они могут устанавливаться на компьютер прямиком с сайта, что обеспечивает более широкое взаимодействие ПК с веб-ресурсом. Соответственно, если элемент вредоносный, он может нанести немалый ущерб компьютеру, на который будет инсталлирован. Если в элементах ActiveX нет необходимости (чаще всего они используются в браузерных играх), их также можно отключить.

Плагины сторонних разработчиков. По частоте проявления это второй после скриптов вид браузерной угрозы. Легальные плагины добросовестных авторов могут существенно облегчить и улучшить работу с браузером, но порой вдобавок к плагину пользователь устанавливает какой-либо шпионский модуль или троянскую программу. Основная опасность в ситуации, когда вредоносное ПО попало в обозреватель Интернета, — это потеря брандмауэром контроля над сетью. Обычно браузер имеет полный доступ к сети, а через него и плагин-троянец или шпион получают возможность пользоваться сетевыми соединениями практически без ограничений. Поэтому оптимальным будет не рисковать и не устанавливать никаких надстроек в браузер или пользоваться только фирменными надстройками с сайтов разработчиков.

5.2. Методы маскировки вредоносных файлов

Если вирус легко обнаружить — это плохой вирус. К сожалению, вредоносное ПО стараются делать на совесть во всем, в том числе, старательно прорабатывая механизм маскировки. Существует два принципиальных метода скрытия вируса в системе:

- Автоматическая маскировка — руткит-технологии (от англ. Root kit — загрузочный пакет) и подмена системных файлов.

- Ручная маскировка — сюда относятся все приемы «ручного» скрытия вируса в системе.

Рассмотрим эти методы подробнее.

5.2.1. Автоматическая маскировка

1. Руткит-технологии

Суть этого метода маскировки в том, что вредоносная программа перехватывает запросы операционной системы и подменяет их. Так, она может, например, «подставлять» антивирусной программе правильные данные о проверяемых файлах, в то время когда эти файлы уже безнадежно испорчены. Разумеется, это возможно только в случае, когда антивирус не имеет антируткит-функции. Руткиты делятся на два вида по принципу действия:

- изменяющие алгоритмы выполнения системных функций (Modify execution path),
- изменяющие системные структуры данных (Direct kernel object manipulation),

и на два типа по уровню воздействия:

- уровня пользователя (user-mode),
- уровня ядра (kernel-mode).

Руткит — полноценный компонент вируса, но сам он ничего, кроме как скрывать деятельность вредоносной части вируса, не может.

2. Подмена системных файлов

Зачастую вирус не только поражает какие-либо данные, но сперва подменяет собой системные файлы. То есть в зараженной ОС часть важных файлов представляют собой вирусы, способные выполнять базовые функции системных элементов. Такое встречается достаточно редко, поскольку требует от вирусописателя хороших навыков в программировании. Чтобы выявить подмену, можно проверить действительность цифровой подписи файла или его контрольную сумму (md5) файла. Работа с контрольными суммами и цифровыми подписями описана далее.

5.2.2. Ручная маскировка

Эти методы не столь эффективны, как руткит-технология, зато технически несравнимо проще, что и сделало их столь популярными. Рассчитана эта маскировка, прежде всего, на невнимательных системных администраторов и пользователей, имеющих слабое представление о компьютерной безопасности. Вот основные средства подобной системы скрытия:

Маскировка вредоносного ПО под файлы операционной системы. Здесь существуют два основных варианта:

1. Вирусу дается имя одного из системных файлов, но размещается он в другой папке, нежели настоящий системный файл. Чаще всего мишенями подлога становятся файлы svchost.exe, winlogon.exe, lsass.exe и другие. В таблице приведено стандартное расположение системных файлов Windows, наиболее часто подделываемых злоумышленниками. Если эти файлы встречаются в других папках (в том числе системных) — это вирусы.

Файл	Расположение
Svchost.exe	C:\WINDOWS\system32
Winlogon.exe	C:\WINDOWS\system32
lsass.exe	C:\WINDOWS\system32
userinit.exe	C:\WINDOWS\system32
ipconfig.exe	C:\WINDOWS\system32
mmc.exe	C:\WINDOWS\system32
services.exe	C:\WINDOWS\system32

shutdown.exe	C:\WINDOWS\system32
winspool.exe	C:\WINDOWS\system32
tcpip.sys	C:\WINDOWS\system32\drivers
explorer.exe	C:\WINDOWS
TASKMAN.EXE	C:\WINDOWS

2. Имя вируса или троянца делают визуально похожим на имя системного файла. Этого добиваются двумя методами: добавляют или убирают один-два символа или используют буквы в различных национальных кодировках (например, добавляются русские или немецкие буквы, схожие внешне с латинскими). Уже несколько лет вирусы чаще всего маскируются под файл svchost.exe. Создан даже своеобразный «топ» подделок:
   1. svchost.exe (вместо английской «c» используется русская «c»)
   2. svchost.exe (вместо английской “o” используется русская “o”)
   3. svcchost.exe (2 “c”)
   4. svhost.exe (пропущено “c”)
   5. svch0st.exe (вместо “o” используется ноль)
   6. svchos1.exe (вместо “t” используется единица)
   7. svchosl.exe (вместо “t” используется “l”)
   8. svchosts.exe (в конец добавлено “s”)
   9. svchoste.exe (в конец добавлено “e”)
   10. svchostt.exe (две “t” на конце)
   11. svchost32.exe (в конец добавлено “32”)
   12. svchosts32.exe (в конец добавлено “s32”)
   13. svchosthlp.exe (в конец добавлено “hlp”)
   14. svdhost32.exe (вместо “c” используется “d” + в конец добавлено “32”)
   15. svshost.exe (вместо “c” используется “s”)
   16. svehost.exe (вместо “c” используется “e”)
   17. svrhost.exe (вместо “c” используется “r”)
   18. svchest.exe (вместо “o” используется “e”)
   19. svschost.exe (после “v” добавлено лишнее “s”)
   20. svcshost.exe (после “c” добавлено лишнее “s”)
   21. svxhost.exe (вместо “c” используется “x”)
   22. syshost.exe (вместо “vc” используется “ys”)
   23. svchoes.exe (вместо “st” используется “es”)
   24. svhostes.exe (пропущено “c” + в конец добавлено “es”)
   25. ssvvcchhoosst.exe (все символы имени продублированы)

Почему svchost.exe? Дело в том, что этот файл является основным для запуска всех системных служб, которые стартуют из динамически загружаемых библиотек (.dll), то есть в памяти всегда находится несколько процессов с этим названием, что позволяет достаточно легко замаскировать вирус среди них (в то же время у каждого запущенного через svchost процесса свой идентификатор). Поэтому к данному файлу нужно относиться наиболее внимательно, но и с другими тоже расслабляться не стоит.

3. Иногда вредоносное ПО мимикрирует не под системные файлы, а под наиболее распространенные драйвера. Например, под драйвера производителей видеоадаптеров — Nvidia и ATI Radeon. Чтобы вычислить такие вирусы, достаточно посмотреть список служебных файлов на сайте производителя оборудования.
4. Кроме «фокусов» с именем, злоумышленники могут также подделать цифровую подпись или описание файла.

Для просмотра описания файла достаточно навести на него курсор мыши. Если какой-то системный файл находится не на своем месте, но описание гласит, что это компонент Windows, — достаточно посмотреть в сети, действительно ли файл с таким именем является указанным в его описании компонентом, или информация фальшивая.

Есть три действенных метода «демаскировки» подозрительных файлов:

- Если вы не уверены, что имя не содержит национальных символов, нажмите правой кнопкой мыши на файл. Выберите в открывшемся меню пункт *Переименовать*, после чего вставьте скопированное в буфер обмена имя в любой текстовый редактор с функцией проверки орфографии. Если имя написано на разных языках, «неправильная» буква будет выделена.
- Проверьте цифровую подпись файла. Для этого нужно нажать на файл правой кнопкой мыши и в контекстном меню выбрать *Свойства*, затем в открывшемся окне перейти на вкладку *Цифровые подписи* и посмотреть *Сведения*. Если в окне сведений значится *Эта цифровая подпись действительна*, то все в порядке. В противном случае файл, вероятнее всего, изменен или подменен.
- Если вы подозреваете, что подпись файла фальшива, или файл не тот, которым пытается притвориться, — можно проверить его контрольную сумму (md5). Для получения контрольной суммы воспользуйтесь программой Hash или ссылкой *http://forum.drweb.com/hash*. При переходе по ссылке укажите нужный файл с помощью кнопки *Обзор*, после чего нажмите *Compute*. Когда анализ завершится, вам будет выдана вся информация о файле, в том числе md5. После этого можно сравнить результат с данными на официальном сайте производителя файла и определить, настоящий он или фальшивый. Для проверки md5 конкретного файла достаточно ввести его контрольную сумму в форму на сайте: *http://fileadvisor.bit9.com/services/search.aspx*.

5.3. Борьба с Autoruns с помощью системной утилиты MSConfig

В ОС Windows есть очень простая и в то же время удобная утилита для работы с системными файлами и настройками. Она называется MSConfig (запуск: *Пуск –> Выполнить –> MSConfig, OK*) и является по сути интерфейсом для просмотра и редактирования ini-файлов. Она может значительно ускорить процесс поиска загрузочных вирусов.

Работать с этой утилитой мы будем по той причине, что через нее можно очень легко отключить автозапуск приложений из системных файлов. Вот какие вкладки программы нам будут интересны:

5.3.1. Вкладка Общие

Здесь можно задать вариант загрузки системы, причем система будет загружаться с указанными параметрами до тех пор, пока они не будут вновь изменены.

Варианты запуска:

Обычный запуск — в этом режиме обрабатываются все ключи автозапуска, папка Автозагрузки, а также запускаются все стандартные драйвера и службы. Установлен по умолчанию, и в отсутствии проблем включать другой режим не рекомендуется.

Диагностический запуск — загружаются только необходимые драйвера и службы. Использовать не рекомендуется — определить источник ошибки будет трудно, поскольку отключается множество драйверов и служб.

Выборочный запуск — позволяет указать, какие системные файлы конфигурации обрабатывать. Отключая по очереди пункты этого меню, можно вычислить, что является причиной сбоев и ошибок и, возможно, примерно определить место расположения поразившего систему вируса.

5.3.2. Вкладка WIN.INI

На этой вкладке в структурированном виде представлено содержимое файла Win.ini (расположен: C:\Windows). Изначально в нем нет строк автозапуска, но они могут быть добавлены туда вирусом и, следовательно, обрабатываться системой. Обратить внимание следует на строки "load" и "run", и соответствующие им значения — имена загружаемых файлов. Для отключения запуска через эти параметры достаточно выделить строку в окне MSConfig и нажать Отключить или просто убрать флажок с соответствующей строки.

5.3.3. Вкладка SYSTEM.INI

Здесь в аналогичном предыдущему файлу формате представлен System.ini (расположен: C:\Windows). Нам будет важен параметр "Shell" раздела "boot", по умолчанию отсутствующий, но который при необходимости может быть создан (вирусом в том числе). Если в этом параметре есть что-то, кроме "Explorer.exe", то, скорее всего, это указание на автозапуск вредоносного ПО. Отключив обработку этого параметра можно заблокировать старт вирусов из данного системного файла.

5.3.4. Вкладка Автозагрузка

На этой вкладке перечислены все программы, запускаемые из различных веток реестра ключами "run" и "load". В графе *Расположение* указано, из какого именно ключа реестра запускается указанный файл. Если здесь обнаружилось какое-либо нелегально запускаемое приложение, его запуск можно отключить, сняв соответствующий флажок, но удалить запись нельзя. Для удаления ключа автозапуска воспользуйтесь редактором реестра Regedit.

Второе средством для борьбы с autorun-вирусами — редактор системного реестра Regedit, который уже неоднократно упоминался выше. Работать с ним не сложно, в случае возникновения вопросов воспользуйтесь встроенной справкой по редактору (*Пуск –> Выполнить –> regedit, OK. Затем выбрать пункт меню Справка –> Вызов справки*).

6. Борьба с вредоносным ПО с помощью Антивируса Dr.Web

В этой главе мы рассмотрим использование антивируса Dr.Web, то есть ситуацию, когда пакет был установлен на компьютер, где ранее никакой защиты установлено не было. Второй вариант ситуации — когда антивирус установлен на инфицированный ПК с целью лечения вирусов и постоянной дальнейшей защиты (подробное описание установки можно прочитать по ссылке: *http://download.drweb.com/doc*, в разделе *Установка антивируса*).

Итак, антивирус установлен, и требуется проверить ПК на вирусы, и, при необходимости, устранить все найденные угрозы.

6.1. Порядок работы с антивирусом

Когда антивирус будет полностью подготовлен к работе (установлен, обновлен, после чего ПК потребуется перезагрузить), в области уведомлений появится фирменный логотип Dr.Web — зеленый паучок. Отсутствие на значке дополнительных элементов (значок красный или с восклицательным знаком) говорит о том, что все установленные компонента антивируса исправны и функционируют, а вирусные базы обновлены. Также паучок свидетельствует о том, что включена постоянная защита ПК от вирусов. В такой ситуации, при попытке какой-либо вредоносной программы активно проявить себя в системе, вирус будет обнаружен и обезврежен. Но неактивные вирусы, даже если они находятся в оперативно памяти, найдены не будут. Наша задача — полностью просканировать компьютер и устранить все опасные программы. Для ее решения нужно выполнить следующие шаги:

1. Нажмите правой кнопкой мыши на значок в области уведомлений и выберите *Сканер*.
2. Когда сканер запустится, выберите пункт *Быстрая проверка* и нажмите *Начать проверку*. В этом режиме сканируется оперативная память и базовые компоненты системы. Если вирусы найдены — выполните действия, указанные в шаге 4.
3. Когда быстрая проверка завершится, можно задать новую проверку. В общем случае все установленные по умолчанию настройки подходят для работы, поэтому требуется только задать объект сканирования и запустить проверку. Поскольку мы подозреваем (или есть уверенность), что какие-либо файлы на ПК заражены, в окне сканера следует отметить флажком пункт *Полная проверка* и нажать кнопку с зеленой стрелкой (*Начать проверку*) под фирменным логотипом Dr.Web.
4. Если в ходе работы сканер обнаружит вирусы — от них необходимо избавиться. В нижней части окна программы будет выведен список зараженных объектов, которые можно с помощью соответствующих кнопок *Вылечить*, *Переименовать*, *Переместить* или *Удалить*. Пораженные файлы рекомендуется попробовать вылечить, если лечение не удалось — удалить. Если часть объектов невозможно вылечить, антивирус переместит их в карантин (они будут скопированы в папку карантина — C:\Program Files\DrWeb\infected!!!). Помещенные в карантин подозрительные объекты можно затем отправить в антивирусную лабораторию «Доктор Веб».

Примечание. Если вы обратитесь за помощью в техническую поддержку Dr.Web, у вас могут попросить лог работы антивируса. Для создания полного отчета воспользуйтесь утилитой Dr.Web SysInfo, подробнее о ней в разделе 10.

Примечание. Антивирусный сканер — это возможность «заставить» Dr.Web проверить нужный вам объект. Постоянную защиту ПК обеспечивает другой компонент — антивирусный сторож SpIDer Guard.

7. Лечение системы с помощью лечащей утилиты Dr.Web CureIt!

Лечащая утилита Dr.Web CureIt! от «Доктор Веб» — первейшее антивирусное средство, с помощью которого необходимо попытаться исцелить ПК от вирусов. Dr.Web CureIt! не требует установки, может запускаться с флеш-накопителя и работает без конфликтов с установленными резидентными антивирусами.

В отличие от полноценного продукта Антивирус Dr.Web, Dr.Web CureIt! представляет собой сканер с набором вирусных баз, что делает его весьма мобильным, но не предоставляет пользователю постоянной резидентной защиты, поскольку сторож SpIDer Guard в пакет Dr.Web CureIt! не входит. Также программа не имеет планировщика и модуля обновления, но модуль самозащиты в утилите присутствует.

Dr.Web CureIt! невозможно обновить — перед использованием необходимо скачать актуальную версию программы с сайта «Доктор Веб» по ссылке: *http://www.freedrweb.com/cureit/?lng=ru*. Важно заметить, что при каждом скачивании генерируется новый дистрибутив утилиты, поэтому, сохраняя Dr.Web CureIt! на жесткий диск, запомните, какое имя имеет файл. Название генерируется из случайной последовательности латинских букв и цифр, но пиктограмма файла — всегда фирменный знак Dr.Web.

Dr.Web CureIt! бесплатна только для домашнего использования, поэтому, если необходимо пролечить чужой компьютер или ПК в офисе, потребуется приобрести лицензию. С условиями лицензирования и приобретения можно ознакомиться по ссылке: *http://www.freedrweb.com/cureit/licensing*.

7.1. Порядок работы с утилитой Dr.Web CureIt!

Ниже мы пошагово разберем алгоритм работы с лечащей утилитой Dr.Web CureIt! на ПК, пораженном вирусами, но не полностью заблокированном (запустить Dr.Web CureIt! на пораженной системе возможно). Для работы нам понадобится только свежий дистрибутив Dr.Web CureIt!. Итак:

1. Скачайте утилиту, запомнив имя и местоположение скачиваемого файла. Если доступ к сайту *http://www.freedrweb.com* заблокирован, скачайте утилиту с другого ПК и на флешке перенесите на свой компьютер.
2. Запустите скачанный файл.
3. Загрузившись, Dr.Web CureIt! временно заблокирует работу системы и выведет на экран информацию о режиме усиленной защиты. Если есть подозрение на присутствие в системе активных вирусов, рекомендуется нажать *OK* и проверить ПК в защищенном режиме. Выходить из этого режима (кнопка *Отмена*) имеет смысл, только если проверка проводится с профилактическими целями в фоновом режиме.
4. Появится окно с краткой информацией о лицензировании. Можно ознакомиться с условиями покупки, выбрав *Да*, но если лечение требуется немедленно, и оно не противоречит лицензионному соглашению, нажмите *Нет.*
5. Откроется окно с двумя вариантами действий:
   - Пуск
   - Обновить

   Поскольку скачивается всегда последняя версия, нажмите *Пуск.*

   Примечание. Если ваш дистрибутив был выпущен более суток назад, будет выведено окно с предупреждением, что программу необходимо обновить.

   Примечание. После проверки системы Dr.Web CureIt! рекомендуется удалить с жесткого диска, а при необходимости повторной проверки — скачать новую версию.
6. Dr.Web CureIt! предложит провести быструю проверку на вирусы. Нажатие кнопки *Нет* откроет предыдущее окно, поэтому необходимо выбрать *Да*. Начнется сканирование основных элементов системы. Если планируется выполнение полной проверки ПК, лучше не тратить время на быструю — нажатием кнопки с зеленым квадратом (*Остановить проверку*) сканирование можно прервать. Если утилита запущена для профилактики — дождитесь окончания проверки.
7. Во время работы программы может появиться зеленое окошко с предложением бесплатно попробовать полную версию антивируса Dr.Web. При работе в обычном режиме это можно сделать немедленно, перейдя по ссылке в окне. Если демоверсия не требуется, закройте диалоговое окно.
8. Когда быстрая проверка будет закончена или остановлена, вы увидите рабочее окно программы. В общем случае все установленные по умолчанию настройки подходят для работы, поэтому требуется только задать объект сканирования и запустить проверку. При подозрении, что ПК инфицирован, следует выбрать пункт *Полная проверка* и нажать кнопку с зеленой стрелкой (*Начать проверку*) под фирменным логотипом Dr.Web.

   Примечание. Более подробно о программе Dr.Web CureIt! и ее настройках можно прочитать в меню *Помощь –> Разделы помощи*.
9. Если в ходе работы Dr.Web CureIt! обнаружит вирусы — от них необходимо избавиться. В нижней части окна программы будет выведен список зараженных объектов, которые можно с помощью соответствующих кнопок *Вылечить*, *Переименовать*, *Переместить* или *Удалить*. Пораженные файлы рекомендуется попробовать вылечить, если лечение не удалось — удалить. Если часть объектов невозможно ни вылечить, ни удалить, необходимо либо переместить файлы (они будут скопированы в папку карантина по адресу C:\Documents and Settings\Ваше_имя_пользователя\DoctorWeb\Quarantine), либо переименовать их. Переименование может потребоваться, чтобы при повторном запуске утилита смогла удалить пораженные файлы, поскольку стереть объекты, в данный момент используемые системой, невозможно. Помещенные в карантин подозрительные объекты можно затем отправить в антивирусную лабораторию «Доктор Веб».

Примечание. Если вы обратитесь за помощью в техническую поддержку Dr.Web, у вас могут попросить лог работы программы Dr.Web CureIt! для анализа. Отчет утилиты (log-файл) находится в папке C:\Documents and Settings\Ваше_имя_пользователя\DoctorWeb\ и называется CureIt.log.

Примечание. Если HOSTS файл был изменен, Dr.Web CureIt! выдаст соответствующее предупреждение с предложением восстановить его в исходное состояние. Если изменения в HOSTS вносились вами или системным администратором, необходимо нажать Нет, в противном случае нажатием кнопки Да приведите файл в порядок.

Примечание. Использование Dr.Web CureIt! — лишь разовая мера спасения, которую вы можете использовать в экстренной ситуации, но она не заменит полнофункционального антивируса. Чтобы всегда быть уверенным в безопасности своего ПК, используйте полный антивирусный пакет Dr.Web.

8. Лечение и восстановление системы с помощью Dr.Web LiveCD/USB

Средства аварийного восстановления системы Dr.Web LiveCD и Dr.Web LiveUSB — это продукты компании «Доктор Веб», позволяющие загрузить ПК со сменного носителя (компакт-диска или флеш-накопителя). Загрузив компьютер, вы сможете провести антивирусную проверку с помощью интегрированного в состав пакета антивируса и удалить все вредоносные объекты из системы, а также извлечь критически необходимые данные. В нашем примере мы рассмотрим процесс работы с Dr.Web LiveCD, поскольку, не считая этапов загрузки, эти продукты функционируют одинаково.

8.1. Создание загрузочного носителя

Dr.Web LiveCD. Для создания загрузочного компакт-диска скачайте iso-образ Dr.Web LiveCD по ссылке: *http://download.geo.drweb.com/pub/drweb/livecd/drweb-livecd-600.iso*. Затем с помощью любой программы для прожига CD запишите образ на чистый компакт-диск. Например, если вы используете Nero Burning ROM, вам необходимо сделать следующее:

- Вставить чистый CD в привод (привод должен поддерживать функцию прожига).
- В главном меню программы выбрать Файл –> Открыть.
- В открывшемся окне выберите сохраненный образ.
- Нажать кнопку Прожиг и дождаться окончания процесса записи.

Примечание. Записать образ Dr.Web LiveCD можно только на CD-диск, DVD не подходит.

Dr.Web LiveUSB. Для создания загрузочной флеш-карты скачайте дистрибутив Dr.Web LiveUSB (по ссылке:) и запустите загруженный файл, предварительно присоединив к компьютеру флеш-накопитель. В открывшемся окне укажите, какую флешку нужно использовать (если их несколько), и требуется ли ее перед этим форматировать. Нажмите *Создать Dr.Web LiveUSB* и дождитесь окончания процесса. Когда создание будет завершено — нажмите *Выход*.

8.2. Загрузка со сменного носителя

В большинстве современных ПК и ноутбуков есть клавиша, которая позволяет выбрать загрузку с любого носителя, который имеется в компьютере. Как правило, эта клавиша F11. При ее нажатии появляется меню с выбором устройства загрузки. В более старых версиях BIOS устройство загрузки можно выбрать вручную. Для этого необходимо зайти в BIOS, при загрузке нажав кнопку Del или F2, затем открыть раздел загрузки *Boot Settings* (иногда просто *Boot*) и поменять последовательность загрузки. Для Dr.Web LiveCD первым пунктом необходимо поставить *CD-ROM*, для Dr.Web LiveUSB — *USB* или *Removable device*.

В начале загрузки с Live-устройства на экран будет выведено меню с вариантами запуска. Как правило, достаточно просто нажать клавишу Enter, так как вариант по умолчанию (Dr.Web LiveUSB (Default)) — самый простой и наглядный. С ним мы и будем работать.

Примечание. Иногда ПК может загрузиться с флеш-карты, только если в настройках BIOS она указана как первичный жесткий диск. В этом случае внесите необходимые коррективы в BIOS и перезагрузите компьютер.

8.3. Проверка системы

Когда загрузка будет завершена, вы увидите рабочий стол, схожий с рабочим столом Windows. Автоматически запустится приложение *Dr.Web Control Center для Linux*. Для полной проверки ПК на вирусы необходимо выполнить следующие действия:

- В программе *Dr.Web Control Center для Linux* откройте вкладку *Сканер (Scanner)*.

- В открывшемся окне в разделе *Режим сканирования (Scan modes)* выберите пункт *Полное сканирование (Full Scan)*.
- Нажмите кнопку *Начать сканирование (Begin to scan)*.
- Если во время сканирования будут обнаружены зараженные объекты, выделите их и укажите, какое действие сканер должен выполнить в списке *Действия (Select objects from the list and apply a relevant action)*. Сначала файлы нужно попробовать *Вылечить (Cure)*, если лечение невозможно, их нужно либо *Удалить (Delete)* либо *Переместить в карантин (Move to quarantine)*.

Закончив работу, закройте сканер и перезагрузите ПК. Для перезагрузки нажмите на значок Dr.Web в левом нижнем углу экрана (на месте стандартной кнопки *Пуск*) и в открывшемся меню выберите пункт *Перезагрузка (Restart)*. Внесите изменения в BIOS, чтобы ПК загружался с жесткого диска, и проверьте, восстановлено ли функционирование системы.

Если удаление вирусов не помогло вернуть компьютер в рабочее состояние, попробуйте исправить реестр, как описано в разделе 7.

8.4. Резервное копирование важных данных

Если есть необходимость извлечь с поврежденного ПК какие-либо важные файлы или папки, их можно скопировать на флеш-накопитель (его необходимо вставить ДО загрузки ПК).

Для копирования файлов сделайте следующее:

- Запустите *Midnight Commander* с помощью ярлыка на рабочем столе. Интерфейс этой программы прост и интуитивно понятен, внешне он практически не отличается от известного большинству пользователей *Norton Commander*.
- В окне программы перейдите в корневой каталог, нажав на символ перехода в родительский каталог «/..», в заголовке левого столбца появится значок «/».
- Перейдите в каталог /WIN, в нем отображаются буквы жестких дисков вашего ПК. Откройте нужный диск (например: /D), а затем каталог, содержимое которого нужно скопировать на флешку.
- С помощью клавиши Tab перейдите в правую колонку файлового менеджера и описанным ранее способом откройте корневой каталог флеш-накопителя (например: /F).
- Вернитесь в левую колонку и с помощью клавиши F5 скопируйте нужный файл или папку на флеш-носитель. Аналогичным методом можно скопировать остальные файлы и папки.

Примечание. *Описанным выше способом можно извлечь файлы реестра и, экспортировав их на другой ПК, исправить и восстановить в рабочее состояние, что позволит вернуть систему в рабочее состояние (подробнее см. в разделе 7).*

9. Поиск вирусов с помощью Shark-режима сканера Dr.Web

9.1. Shark–режим сканера

Версия 6.0 антивирусного сканера Dr.Web, предназначенная для 32-битных систем, имеет встроенный антируткит-движок Shark, работающий на основе антируткита Dr.Web Shield. В Shark-режиме сканер производит сбор информации о системе и полностью автономен — для его работы не требуются лицензионный ключ и вирусные базы.

Как можно использовать этот режим для борьбы с вирусами, если Shark-сканирование не лечит вирусы? Ответ состоит в том, что созданный сканером отчет позволяет вручную проанализировать состояние системы и обнаружить вирусную активность, независимо от того, присутствует запись о вирусе в базах антивируса или нет. После обнаружения подозрительных файлов можно отправить их на анализ в лабораторию компании «Доктор Веб» или просто удалить, если есть твердая уверенность, что это именно вирусы.

Принцип работы Shark-сканера совпадает с принципом работы антируткита Shield — устанавливаясь как драйвер, он перехватывает все функции, тем самым отслеживая потоки данных и перехваты, что позволяет выявить руткиты и скрытые процессы. Подробнее о технологиях перехвата можно прочитать здесь: *http://ru.wikipedia.org/wiki/Перехват_(программирование)*.

Пользоваться Shark-режимом можно, даже если антивирус Dr.Web отсутствует на компьютере. Скачайте последнюю версию лечащей утилиты Dr.Web CureIt! и используйте встроенный в нее сканер.

9.2. Получение отчета Shark–режима

Для запуска Shark-режима необходимо сделать следующее:

- ***Если у вас установлен антивирус Dr.Web.*** Нажмите *Пуск –> Выполнить*, в строку введите *drweb32w /shark* и нажмите *OK*.
- ***Если антивируса Dr.Web на ПК нет.*** Скачайте лечащую утилиту Dr.Web CureIt! и сохраните ее в корневую папку диска C: (для простоты запуска). Затем нажмите *Пуск–> Выполнить*, в строку введите *C:\имя_дистрибутива_cureit /shark* и нажмите *OK*.

Появление на экране фирменной заставки Dr.Web свидетельствует, что сканирование началось. Подождите, пока заставка не исчезнет — это будет говорить о завершении проверки. В среде Windows XP созданный программой отчет будет находиться по адресу *C:\Documents and Settings\Ваше_имя_пользователя\DoctorWeb\drweb32w.log* (если антивирус Dr.Web установлен) или *C:\Documents and Settings\Ваше_имя_пользователя\DoctorWeb\CureIt.log* (если Shark-режим запускался с помощью Dr.Web CureIt!). В Windows Vista и Windows 7 отчет располагается в папке *C:\Users\ Ваше_имя_пользователя\DoctorWeb\drweb32w.log* (если антивирус Dr.Web установлен) или *C:\Users\Ваше_имя_пользователя\DoctorWeb\CureIt.log* (если Shark-режим запускался с помощью Dr.Web CureIt!). Открыть отчет можно с помощью любого текстового редактора.

Примечание. На компьютерах с малым (<512 Мб) объемом оперативной памяти создание log-файла может занять длительное время (более получаса).

9.3. Анализ отчета

Теперь, когда у вас есть отчет, сформированный Shark-режимом сканера, можно приступать к анализу процессов, происходящих в системе, и поиску следов вирусной активности. Для примера мы разберем отчет, сформированный сканером на компьютере одного из пользователей, обратившегося в службу технической поддержки.

Отчет Shark-режима начинается строкой:

********** SHARK REPORT **********

Далее идут разделы проверки:

Processes IAT/EAT/Splicing. Проверка импортов (IAT)/экспортов (EAT)/перехвата кода (Splicing, читается сплайсинг) в процессах и загруженных в них dll. Для каждой dll, спроецированной в адресное пространство процесса, и самого образа (.exe) осуществляется проверка импортируемой и экспортируемой таблиц адресов и секций с кодом. Наличие информации в этой секции говорит о том, что какой-то код (легальный или руткит) внес изменения в выполнение программы. Первым идет проверка перехвата кода (сплайсинг):

[SPLICING CHECKING]
Process: 1768 (spiderml.exe)
MODULE: C:\WINDOWS\system32\kernel32.dll
SECTION: .text
ADDRESS: 7C8449FD
NAME: SetUnhandledExceptionFilter+0
COUNT: 5 => JMP 004038A0 (C:\Program Files\DrWeb\spiderml.exe)

В данном процессе стоит перехват в коде kernel32.dll, на функции SetUnhandledExceptionFilter, причем перехват поставил сам же модуль. Ничего страшного в этом нет.

[IAT CHECKING]
Process: 1440 (explorer.exe)
FUNCTION explorer.exe->KERNEL32.dll!GetProcAddress
HOOKED 5CB77774 (C:\WINDOWS\system32\shimeng.dll)
[IAT CHECKING]
Process: 1440 (explorer.exe)
FUNCTION netapi32.dll->KERNEL32.dll!GetProcAddress
HOOKED 5CB77774 (C:\WINDOWS\system32\shimeng.dll)

В процессе explorer.exe в импорте netapi32.dll, где импортируется функция GetProcAddress в KERNEL32.dll, стоит перехват библиотеки shimeng.dll. Найдя файл в указанной папке, можно проверить его цифровую подпись. Она гласит: *Shim Engine DLL, Microsoft Corp.* Вывод: не руткит.

Проверить, является ли файл подлинным, можно по его контрольной сумме (параметрам MD5, SHA-1 и SHA-256), пройдя по ссылке *http://www.virustotal.com/search.html* и введя один из этих параметров в строку поиска. После нажатия кнопки search будут выведены результаты поиска данной контрольной суммы в базах данных производителей антивирусов. Кроме того, можно сверить полученную контрольную сумму с данными из сети. Например, на сайте *http://www.dll.ru/dll.html* есть контрольные суммы огромного количества dll-файлов различных производителей. Там же можно скачать новый файл взамен поврежденного.

Ниже приведен пример перехвата кода на машине, зараженной вирусом TDL3:

[SPLICING CHECKING]
Process: 1048 (svchost.exe)
MODULE: C:\WINDOWS\system32\mswsock.dll
SECTION: .text
ADDRESS: 71A54057
COUNT: 5 => JMP 047F000C (unknown)
[SPLICING CHECKING]
Process: 1048 (svchost.exe)
MODULE: C:\WINDOWS\system32\mswsock.dll
SECTION: .text
ADDRESS: 71A5433A
COUNT: 5 => JMP 0478000C (unknown)
[SPLICING CHECKING]

Process: 1048 (svchost.exe)
MODULE: C:\WINDOWS\system32\mswsock.dll
SECTION: .text
ADDRESS: 71A5583F
COUNT: 5 => JMP 047E000C (unknown)
[SPLICING CHECKING]
Process: 1364 (explorer.exe)
MODULE: C:\WINDOWS\system32\mswsock.dll
SECTION: .text
ADDRESS: 71A54057
COUNT: 5 => JMP 00B7000C (unknown)
[SPLICING CHECKING]
Process: 1364 (explorer.exe)
MODULE: C:\WINDOWS\system32\mswsock.dll
SECTION: .text
ADDRESS: 71A5433A
COUNT: 5 => JMP 00B5000C (unknown)

Нелегальный перехват кода в библиотеке mswsock.dll, в процессах svchost.exe и explorer.exe.

Drivers IAT/EAT/Splicing. Проверка импортов (IAT)/экспортов (EAT)/перехвата кода (Splicing) в драйверах. Если у драйвера перехвачено много импортов, это может говорить о том, что просто включен Verifier (системное средство проверки подлинности драйверов Verifier.exe, подробнее о нем можно прочитать по ссылке: *http://support.microsoft.com/kb/244617*).

[SPLICING CHECKING]
Driver: c:\windows\system32\vmx_fb.dll
SECTION: .text
ADDRESS: BF9D6ED0
COUNT: 5 => JMP F960D9A0 (siwvid.sys)

У драйвера vmx_fb.dll стоит перехват в коде, который ведет в siwvid.sys (SIWVID.sys — legacy video support, NuMega Lab) драйвер отладчика SoftICE, по поведению очень похожий на руткит. Файл нужно отправить на анализ.

[SPLICING CHECKING]
Driver: c:\windows\system32\vmx_fb.dll
SECTION: .text
ADDRESS: BF9B9ED0
COUNT: 5 => JMP F83B59A0 (siwvid.sys)
[SPLICING CHECKING]
Driver: c:\windows\system32\vmx_fb.dll
SECTION: .text
ADDRESS: BF9BA01C
COUNT: 5 => JMP F83B59D6 (siwvid.sys)

В случае с работающим Verifier, у драйверов, которые добавлены для проверки, будут перехвачены импорты. В таком случае это тоже не следствие действий руткита.

[IAT CHECKING]
Driver: C:\WINDOWS\System32\drivers\ntfs.sys
FUNCTION ntoskrnl.exe!KeReleaseMutant
HOOKED 8063DD2D (\WINDOWS\system32\ntoskrnl.exe)
[IAT CHECKING]
Driver: C:\WINDOWS\System32\drivers\ntfs.sys
FUNCTION ntoskrnl.exe!KeWaitForSingleObject

HOOKED 8063DC6C (\WINDOWS\system32\ntoskrnl.exe)

В данном случае Verifier настроен на проверку ntfs.sys. В результате у него в IAT функции ядра (ntoskrnl) перехвачены, но ведут в то же ядро, только в другие функции.

[SPLICING CHECKING]
Driver: C:\WINDOWS\System32\drivers\atapi.sys
SECTION: .text
ADDRESS: BAF5D9C8
COUNT: 4
[SPLICING CHECKING]
Driver: C:\WINDOWS\System32\drivers\atapi.sys
SECTION: .text
ADDRESS: BAF5DBD5
COUNT: 4

Очень подозрительная модификация драйвера atapi.sys.

[SPLICING CHECKING]
Driver: c:\windows\system32\win32k.sys
SECTION: .text
ADDRESS: BF8213A9
COUNT: 5 => JMP F93DC69F (\SystemRoot\System32\Drivers\Normandy.SYS)

Безусловный переход в секции .text у user&gdi модуля win32k.sys. Переход ведет в normandy.sys. У драйверов, как и у процессов, возможны множественные сплайсинги, например, если одна из секций или весь файл упакованы. Определение перехватов сплайсинга/IAT/EAT как у драйверов, так и у процессов может показать, насколько легальными методами пользуется ПО для своей работы.

SSDT (System Service Descriptor Table). Проверка модификации SSDT таблиц. Имеет следующий формат:
ID: номер_сервиса NAME: имя_сервиса ADDRESS: адрес_обработчика HOOKED: 1-перехвачен, 0-нет PATH: путь_к_модулю, либо unknown
Пример без перехвата:

ID: 001
NAME: NtAccessCheck
ADDRESS: 805E6DB6
HOOKED: 0
PATH: C:\WINDOWS\system32\ntkrnlpa.exe

В данном случае перехвата нет, адрес указывает на стандартный обработчик в ntkrnlpa.exe (PAE-версия ntoksrnl).
Пример с перехватом:

ID: 001
NAME: NtAccessCheck
ADDRESS: FF60F325
HOOKED: 1
PATH: C:\WINDOWS\system32\sysdrv.sys

Установка перехвата в SSDT — один из самых легких способов маскировки, которыми пользуются руткиты.

Shadow SSDT. Shadow SSDT (Теневая SSDT) — это специальная таблица в win32k.sys, которая содержит адреса системных функций, связанных с отображением пользовательского графического интерфейса (GDI). Формат:

ID: номер_сервиса NAME: имя_сервиса ADDRESS: адрес_обработчика HOOKED: 1-перехвачен, 0-нет PATH: путь_к_модулю, либо unknown
Пример:

ID: 000
NAME: NtGdiAbortDoc
ADDRESS: BF92C1AD
HOOKED: 0
PATH: C:\WINDOWS\system32\win32k.sys

IDT. Проверка таблицы векторов прерываний (англ. Interrupt Descriptor Table, IDT). Раздел имеет формат:

IDT: номер_вектора CPU NO: номер_cpu ADDRESS: адрес_обработчика SYSINT: зарегистрирован_объект_прерывания HOOKED: 1 – перехвачен, 0 – нет PATH: путь_к_обработчику, либо unknown
Н перехваченный элемент имеет вид:

IDT: 098
CPU NO: 001
ADDRESS: F975267E
SYSINT: 1
HOOKED: 0
PATH: C:\WINDOWS\system32\drivers\atapi.sys Перехваченный:
IDT: 001
CPU NO: 001
ADDRESS: F9C1C676
SYSINT: 0
HOOKED: 1
PATH: C:\WINDOWS\system32\drivers\cpthook.sys

Как и в случае с SSDT, перехват определяется флагом HOOKED.

Kernel callbacks. Список callback-функций, которые NT вызывает для уведомления модулей о различных событиях в ядре, например, уведомление о выполнении операций с реестром, завершение работы. Формат:

CALLBACK: CreateProcess
ADDRESS: F75A9CDC
PATH: c:\windows\system32\drivers\vmci.sys

Где:
- CALLBACK–– наименование функции обратного вызова
- ADDRESS–– адрес
- PATH–– путь к месторасположению функции

Пример:

CALLBACK: CreateProcess
ADDRESS: F9BAD428
PATH: c:\windows\system32\drivers\vmdebug.sys
CALLBACK: BugCheck
ADDRESS: 806D77CC
PATH: C:\windows\system32\hal.dll
CALLBACK: BugCheckReason
ADDRESS: F9E78AB8
PATH: c:\windows\system32\drivers\mssmbios.sys

CALLBACK: CmRegistry
ADDRESS: F96F81F6
PATH: C:\Program Files\DrWeb\dwprot.sys
CALLBACK: FsCallback
ADDRESS: F970E876
PATH: C:\WINDOWS\system32\drivers\sr.sys
CALLBACK: SeFileSystem
ADDRESS: F7FCC3CF
PATH: c:\windows\system32\drivers\mrxsmb.sys

Драйвер vmdebug.sys зарегистрирован на уведомление о создании процесса (CALLBACK: CreateProcess), hal.dll – на уведомлении о BSOD (CALLBACK: BugCheck), dwprot.sys – на операции с реестром.

В случае если зарегистрирован неизвестный компонент – код, не входящий ни в один модуль, в элементе PATH: информация не выводится (значение: <:unknown:>), и такая ситуация считается подозрительной.

Loaded drivers. Список загруженных драйверов. Каждый драйвер представлен в виде: ADDRESS: адрес_в_памяти EP: точка_входа SIZE: размер OBPATH: путь_у_диспетчера_объектов PATH: путь_к_файлу (проверка_подписи).
Пример:

ADDRESS: BA4A9000
EP: BA52E904
SIZE: 0008D000
OBPATH: \FileSystem\Ntfs
PATH: C:\WINDOWS\system32\drivers\ntfs.sys
(STATUS: MS_TRUSTED,
DESCR: NT File System Driver,
COMPANY: Microsoft Corporation,
VER: 5.1.2600.5585 (xpsp_sp3_qfe.080422-1455),
MD5: A0857C97770034FD2AF17DC4014B5ABD,
SHA1: 9585A4844C39D4E4C61EE8BD490D8D20E70FE7F3,
SHA256: 3A325399DD8A384F1EEB2340FB5CA54FCE7360C9A02E8ADB6DE2EF3CFD805A92)

Здесь по каждому файлу есть информация с проверкой подписи, hash, доверенности:
- PATH: – путь до драйвера.
- STATUS: – статус доверенности. Статусы бывают:
  - MS_TRUSTED – высшая степень. Это значит, что файл от Microsoft. Подменить этот сертификат практически невозможно.
  - TRUSTED – файл с сертификатом из списка доверенных издателей (около сотни). Тут абсолютной достоверности нет, поскольку используется API и результат может быть фальшивым.
  - NOT TRUSTED – файл с недоверенным сертификатом.
- SIGNER: – организация, выдавшая сертификат.
- DESCR: – описание файла.
- COMPANY: – организация, указанная в качестве владельца драйвера.
- VER: – версия драйвера.
- MD5: – hash MD5.
- SHA1: – hash SHA-1.
- SHA256: – hash SHA-256.

Параметры SHA-1 и SHA-256 – также элементы контрольной суммы файла. Проверить их, аналогично параметру MD5, можно по ссылке *http://forum.drweb.com/hash*.

Drivers dispatches. Расширенная информация о драйверах и системных dll. В том чисе, рабочие процедуры драйверов (driver dispatch), имена их сервисов.
Пример:

OBPATH: \FileSystem\Cdfs
SERVICE: Cdfs
PATH: c:\windows\system32\drivers\cdfs.sys
IRP_MJ_CREATE => cdfs.sys+400 (F9BEC400)
IRP_MJ_CREATE_NAMED_PIPE => ntkrnlpa.exe!IoVolumeDeviceToDosName+68E (804F354A)
IRP_MJ_CLOSE => cdfs.sys+400 (F9BEC400)
IRP_MJ_READ => cdfs.sys+400 (F9BEC400)

В примере приведена информация о драйвере cdfs.sys: путь в пространстве имен диспетчера объектов, имя сервиса, полный путь к файлу и обработчики первых четырех функций.
В случае, когда системный модуль загружен в память, но для него отсутствует объект-драйвер (чаще всего это dll-файл, который используют другие драйверы), информация имеет вид:

OBPATH: <:unknown:>
SERVICE: <:unknown:>
PATH: C:\windows\system32\kdcom.dll
OBPATH: <:unknown:>
SERVICE: <:unknown:>
PATH: C:\windows\system32\bootvid.dll

Object types. Информация об объектах типов и их функциях, которые NT вызывает в различных ситуациях, например, при создании или высвобождении объекта. Функции часто перехватываются как руткитами, так и антируткитами. Формат:

ID: номер ADDRESS: адрес NAME: имя_типа, далее различные процедуры.

Пример:

ID: #1
ADDRESS: 819C8900
NAME: Desktop
OPENPROC: 0x806037D6 (ntkrnlpa.exe!ExInitializePagedLookasideList+248 (806037D6))
CLOSEPROC: 0x806036B4 (ntkrnlpa.exe!ExInitializePagedLookasideList+126 (806036B4))
DELPROC: 0x8060378C (ntkrnlpa.exe!ExInitializePagedLookasideList+1FE (8060378C))
SECURPROC: 0x805EE42E (ntkrnlpa.exe!SeQuerySecurityDescriptorInfo+2E4 (805EE42E))
OKAYCLOSEPROC: 0x8060371A (ntkrnlpa.exe!ExInitializePagedLookasideList+18C (8060371A))

Функции объекта Desktop (рабочий стол) указывают в ядро, ничего подозрительного. На «чистой» системе все процедуры всех объектов указывают в ядро.

Running processes & modules. В этом разделе перечислены все запущенные процессы и используемые ими модули. Разберем на примере:

PID: 00001516
EPROCESS: 8851C728
PATH: C:\WINDOWS\system32\services.exe
(STATUS: MS_TRUSTED,
DESCR: Приложение служб и контроллеров,
COMPANY: Корпорация Майкрософт,
VER: 5.1.2600.5755 (xpsp_sp3_qfe.090206-1316),
MD5: 0AF0D6AF45220ADB9C30B33CFEC41831,
SHA1: BCBD377ABD8C4DF039E5048E681FFC91CEBEEA3F,
SHA256: 06837569216ACB99CB79F1E3475913AF8760AE7BAFA3F279233D51178D72EF19)

IMAGEBASE: 7C800000
SIZE: 00000000000F8000
PATH: c:\windows\system32\kernel32.dll
(STATUS: MS_TRUSTED,
DESCR: Библиотека клиента Windows NT BASE API,
COMPANY: Корпорация Майкрософт,
VER: 5.1.2600.5781 (xpsp_sp3_gdr.090321-1317),
MD5: 7A163D793AF7208E13B0F33864D36438,
SHA1: 78879B9B7DEB5B88A9B492597B1664B34065BFA8,
SHA256: 880EDB25D52A608B522B175AB11B8CA4FBE1A174EAF5908F9A360AC6F4131A6B)

Где:

- PID – PID процесса (англ. Personal IDentificator – персональный идентификационный номер. Он присваивается операционной системой запущенным процессам в текущей сессии работы). Он является уникальным для каждого запущенного процесса. Однако PID сохраняется одинаковым для каждого из процессов только в текущей сессии работы операционной системы. Если компьютер был перезагружен или выключен на время, то после следующей загрузки PID каждому из процессов будет присвоен другой;
- EPROCESS – главная структура процесса (подробнее: http://www.intuit.ru/department/os/osmswin/5/);
- PATH – путь к файлу;
- STATUS – статус доверенности, см. выше;
- DESCR – описание;
- COMPANY – компания – разработчик программы;
- VER – версия файла;
- MD5 – hash MD5;
- SHA1 – hash SHA-1;
- SHA256 – hash SHA-256.

Далее перечислены все модули, используемые процессом. При этом каждому из них соответствует такой же набор описаний.

Running threads and stack. Информация о запущенных потоках и их стеки. Формат:
ID: порядковый_номер ETHREAD: адрес_объекта_ядра CID(id_процесса.id_потока) STARTADDRESS: стартовый_адрес SYSTHREAD: 1 – системный_поток SDT: адрес_SDT_потока (1 – если перехвачена) PRIORITY: приоритет ISWORKER: 1 – системный_рабочий_поток.
Пример:

ID: #1
ETHREAD: 8179F590
CID(984.1000)
STARTADDRESS: kernel32.dll!CreateThread+22 (7C8106E9)
SYSTHREAD: 0
SDT: 80552FA0 (HOOKED: 0)
PRIORITY: 8
ISWORKER: 0
ntkrnlpa.exe!IoSetIoCompletion+2C9 (8056E1B1)
ntkrnlpa.exe!KeReleaseInStackQueuedSpinLockFromDpcLevel+B14 (8053D638)
ntdll.dll!NtRemoveIoCompletion+C (7C90DA2C)
ntdll.dll!RtlAllocateHeap+1C9 (7C91026D)
kernel32.dll!GetModuleFileNameA+1B4 (7C80B713)

В данном случае анормальностью считается перехваченная SDT, то есть HOOKED: 1 и присутствие на стеке строки unknown вместо имени модуля.

Hidden process modules. Скрытые модули в процессах. В нормальном состоянии здесь ничего не должно быть.

Hidden code in kernel memory. Анализатор скрытого кода в ядре. В нормальном режиме здесь ничего не должно быть. При наличии инфекции, например, активного BackDoor.Tdss последних версий, здесь можно увидеть вспомогательные потоки руткита:

HIDDEN CODE IN THREAD:
ETHREAD: 819C8B30
CID(4.48)
STARTADDRESS: ntkrnlpa.exe!ExQueueWorkItem+B2 (80534B32)
MEM ADDRESS: 8193A508

Network connections. Информация о сетевых соединениях. Пример:

LOCAL ADDR: 0.0.0.0
LOCAL PORT: 135
REMOTE ADDR: 0.0.0.0
REMOTE PORT: 4117
STATE: LISTEN
PID: 796
PATH: c:\windows\system32\svchost.exe
(STATUS: MS_TRUSTED,
DESCR: Generic Host Process for Win32 Services,
COMPANY: Microsoft Corporation,
VER: 5.2.3790.3959 (srv03_sp2_rtm.070216-1710),
MD5: C09CCFE81DEC9B162533D7184D705682,
SHA1: 086FC8C82BA9E1F3F764E15FFBE402A6529EF323,
SHA256: 7FFA8F0DB61522E7BE3FF5A380F16644E72ADD873A8A9E4AC01A5FF376910525)

Где:

- LOCAL ADDR — локальный адрес,
- LOCAL PORT — локальный порт,
- REMOTE ADDR — удаленный адрес,
- REMOTE PORT — удаленный порт,
- STATE — состояние соединения,
- PID — PID процесса,
- PATH — путь к процессу,
- STATUS — статус доверенности (см. выше),
- SIGNER: — организация, выдавшая сертификат,
- DESCR: — описание файла,
- COMPANY: — организация, указанная в качестве владельца файла,
- VER: — версия файла,
- MD5: — hash MD5,
- SHA1: — hash SHA-1,
- SHA256: — hash SHA-256.

Autoruns. Здесь перечислены все файлы, находящиеся в автозагрузке, с указанием адресов, откуда они загружаются.
Пример:

PATH: c:\windows\system32\drivers\fs_rec.sys
(STATUS: MS_TRUSTED,
DESCR: File System Recognizer Driver,
COMPANY: Microsoft Corporation,
VER: 5.2.3790.0 (srv03_rtm.030324-2048),
MD5: AEBFF3D810B74971B91B2B77B289A98B,
SHA1: 829C2DEB5BCD4BACC004B03703BA93923E61F176,
SHA256: E2A63B0BEF3E09000A3AD2564D211D8A9EDACD74BDC949AE2F3BD79C0210AA9B)
REGS:HKLM\System\CurrentControlSet\Services\Fs_Rec, Start

Где:

- PATH — путь к процессу,
- STATUS — статус доверенности (см. выше),
- SIGNER: — организация, выдавшая сертификат,
- DESCR: — описание файла,
- COMPANY: — организация, указанная в качестве владельца файла,
- VER: — версия файла,
- MD5: hash MD5,
- SHA1: hash SHA-1,
- SHA256: hash SHA256,
- REGS: ключ реестра, откуда запускается файл.

Disks MBRs. Проверка MBR (англ. Master Boot Record — главная загрузочная запись) у дисков. Сюда попадает информация о буткитах, в том случае, если MBR различаются. Пример нормальной записи:

Disk: \\.\PhysicalDrive0 — MBR OK
Disk: \\.\PhysicalDrive1 — MBR OK

Anomalies analyzer. Анализатор ненормальностей — в данном разделе отображается информация, основанная на анализе всех предыдущих тестов. Этот раздел наиболее интересен, поскольку здесь можно найти все подозрительные файлы с опасными импортами и подозрительные перехваты функций.

Здесь могут оказаться драйверы Microsoft со статусом "File driver packed" или "contain dangerous imports", поэтому для таких случаев нужно проверять подпись драйвера (в списке всех драйверов) на предмет STATUS: NOT TRUSTED, SIGNER: No issuer, No publisher, SIGNATURE: INVALID.

Отчет Shark режима завершается строкой:

****

9.4. Примеры обнаружения известных вирусов

Ниже приведены примеры того, как сканер реагирует на активность некоторых вирусов и как это отображается в отчете:

TDSS для x64 (также известный как TDL4)

Kernel callbacks:

CALLBACK: LoadModule ADDRESS: 8193A1D2 PATH: <:unknown:>

В анализаторе скрытого кода в ядре видны вспомогательные потоки руткита:

Hidden code in kernel memory:

HIDDEN CODE IN THREAD: ETHREAD: 819C8B30 CID(4.48) STARTADDRESS: ntkrnlpa.exe!ExQueueWorkItem+B2 (80534B32) MEM ADDRESS: 8193A508

HIDDEN CODE IN THREAD: ETHREAD: 819C8B30 CID(4.48) STARTADDRESS: ntkrnlpa.exe!ExQueueWorkItem+B2 (80534B32) MEM ADDRESS: 81041800

Зараженный MBR:

Disks MBRs:

Faked mbr: \\.\PhysicalDrive0 – probably active bootkit

ORIG: 33C08ED0BC007C8EC08ED8BE007CBF0006B90002FCF3A450681C....

FAKE: 33C08ED0BC007CFB5007501FFCBE1B7CBF1B065057B9E501F3A4C....

BackDoor.MaosBoot

Disk MBRs:

Faked mbr: \\.\PhysicalDrive0 – probably active bootkit

ORIG: 33C08ED88EC08ED0BC007CBE1A7CBF0006B9E6015057FCF3A4CBBEA407B10490803C80740D382C0F85B90083C610E2F0CD18668B44088B148...

FAKE: 33C08ED0BC007CFB5007501FFCBE1B7CBF1B065057B9E501F3A4CBBDBE07B104386E007C09751383C510E2F4CD188BF583C610497419382C7...

BackDoor.Tdss

Loaded drivers:

ADDRESS: F974D000 EP: F97637A4 SIZE: 00018000 PATH: C:\WINDOWS\system32\drivers\atapi.sys (STATUS: NOT TRUSTED, SIGNER: No issuer:No publisher, SIGNATURE: INVALID, MD5: 50D584ED6A824681127A7D1E837104B0, SHA1: 4E72FB84933DC5376DE89903F3B2BC94E1CF1688, SHA256: 71590551D57E72B8002C478983DABB7BB3AD6E4F5C0D471336BB8AA878D1040B)

ADDRESS: 00000000 EP: 00000000 SIZE: 00000000 PATH: unknown (susplicious driver) (STATUS: NOT TRUSTED, SIGNER: No issuer:No
publisher, SIGNATURE: INVALID)

Anomalies analyzer:

Faked driver file: C:\WINDOWS\system32\drivers\atapi.sys

File driver entry point modified: C:\WINDOWS\system32\drivers\atapi.sys

Faked startup file: c:\windows\system32\drivers\atapi.sys

"Faked driver" означает, что вирус пытается выдать сканеру ложную информацию о том, что записано на диске.

Win32.Ntldrbot (Rustock.C)

Anomalies analyzer:

File driver packed: c:\windows\system32\drivers\ftdisk.sys

10. Анализ системы с помощью утилиты Dr.Web SysInfo

Сервисная утилита Dr.Web SysInfo – хороший инструмент для анализа состояния системы. По отчету, сформированному Dr.Web SysInfo, можно досконально изучить происходящие на ПК процессы и выявить возможные причины нестабильной работы: конфликты оборудования, конфликты программ или вирусную активность.

Утилита полностью бесплатна, скачать ее можно по ссылке: *ftp://ftp.drweb.com/pub/drweb/tools/dwsysinfo.exe*. Для работы Dr.Web SysInfo не требуются никакие дополнительные компоненты, просто запустите скачанный файл (dwsysinfo.exe) и в открывшемся окне нажмите *Сформировать отчет*.

Имя файла отчета может выглядеть, например, так: VD_v_300111_105015.zip. Где VD – имя компьютера, v – имя пользователя, 300111 – дата создания отчета в формате ддммгг, 105015 – время создания отчета в формате ччммсс. Расширение .zip говорит о том, что отчет сжат в архив ZIP-формата. Архив с отчетом сохраняется в папке C:\Documents and Settings\Ваше_имя_пользователя\DoctorWeb. Когда создание архива завершено, программа выводит окно с информацией об имени и месте его расположения.

Примечание. Настройки программы по умолчанию являются оптимальными. При необходимости можно изменить перечень включаемых в анализ элементов системы. Для этого после запуска программы нажмите* Параметры отчета*, отметьте флажками пункты, информация о которых требуется, и выберите* Сформировать отчет*.

Примечание. Кроме архива, программа создает log-файл, в который заносятся описания всех проблем, возникших в ходе работы (например, если какой-то файл не был найден или было отказано в доступе). Он называется SysInfoLog.txt и располагается в папке со сформированным отчетом.

10.1. Анализ отчета Dr.Web SysInfo

При задании сбора полной информации о системе (настроено по умолчанию) архив Dr.Web SysInfo будет содержать следующие файлы:

- Applications.evt
- DrWebInfo.xml
- DrWebRegistryExport.xml
- HOSTS
- msinfo32report.nfo
- System.evt
- DoctorWeb.evt
- SystemInfo.xml
- SystemRegistryExport.xml

Файлы .xml открываются с помощью браузера, файл HOSTS – любым текстовым реактором, .nfo – системной утилитой *Сведения о системе*, .evt – программой *Event Log Explorer* (скачать trial-версию можно по ссылке: *http://www.eventlogxp.com/download/elex.zip*). Содержимое каждого файла мы рассмотрим отдельно:

Applications.evt – журнал событий, созданных различными приложениями. Сюда входят информационные события (Information, например, отчет об успешных обновлениях), предупреждения (Warning, например, когда возникают какие-то конфликты или обнаружено несоответствие прав, что может привести к нарушению защиты) и ошибки (Error, например, «вылет» программы). Все события досконально описываются в графе Description.

DrWebInfo.xml – в разделах этого файла содержится информация о функционирующих в системе компонентах Dr.Web:

LaunchedModules – здесь перечислены компоненты антивируса с их статусами. True – компонент активен, False – компонент отключен или недоступен по лицензии;

LicenceFiles – указывает на лицензионный файл;

DirectoriesListing – перечень файлов папки Dr.Web.

Если антивирус Dr.Web не установлен – в первом разделе везде будет значение False, в других местах не будет ничего.

DrWebRegistryExport.xml – здесь перечислены ветки реестра, отвечающие за функционирование Dr.Web. По большей части эта информация для службы технической поддержки.

Примечание. Файлы DrWebInfo.xml и DrWebRegistryExport.xml используются для диагностики неполадок в самом антивирусе и требуются в первую очередь для инженеров поддержки. При использовании утилиты для поиска следов вирусов они не используются.

HOSTS – копия системного HOSTS файла. Можно сразу проверить его и, при необходимости, удалить все лишнее из оригинального файла в системной папке.

msinfo32report.nfo – это отчет, создаваемый системной утилитой *Сведения о системе* (вызов: *Пуск –> Программы –> Стандартные –> Служебные –> Сведения о системе*). Как пользоваться этой утилитой для диагностики системы поясняется в ее руководстве пользователя (*Справка –> Вызов справки*).

System.evt – системный журнал событий. Здесь можно отследить проблемы, возникающие у системных компонентов и служб. Формат данных аналогичен предыдущему файлу этого типа.

DoctorWeb.evt – журнал событий, зарегистрированных антивирусом. Здесь отображаются все события, связанные с обнаружением подозрительных, инфицированных и непроверенных файлов, а также информация об изменении состояния компонентов (например, выключение/отключение SpIDer Gate и т. д.).

SystemInfo.xml – в этот файл выводится сводка по всем параметрам системы. Он содержит следующие разделы:

- SystemInfo – сведения о компьютере. Сюда входят данные о компонентах системы: ОС, процессор, память, жесткие диски, перечень пользователей, права текущего пользователя, текущее местоположение, системные папки Windows и сетевые адаптеры.
- AntivirusInfo – данные об установленном антивирусе.
- FireWall – данные об установленном в системе брандмауэре. Если установлен только системный брандмауэр, раздел будет пустым.
- ProcessesInfo – информация по всем активным процессам. Самый крупный раздел файла.
- Serviceinfo – здесь перечислены запущенные системные службы.
- DriversInfo – информация об используемых системой драйверах.
- BrowserInfo – данные по установленному по умолчанию браузере.
- InstalledApplications – сведения обо всех установленных приложениях, в том числе обновлениям к продуктам Microsoft (Windows, Office и др.).

SystemRegistryExport.xml – этот файл содержит экспорт наиболее важных веток реестра:

Раздел автозагрузки:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Раздел системных настроек:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services – системные сервисы
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule – планировщик
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot – безопасный режим
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application – журнал событий приложений
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes – сетевые настройки
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment – переменные среды окружения

Прочие параметры:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options – запрет на отображение перечисленных в данной ветке файлов (то есть программу можно запустить, но работать с ней станет невозможно. Например, при добавлении сюда параметра со значением "explorer.exe", вы не увидите рабочего стола).
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon – параметры автозагрузчика.
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows – раздел системных настроек Windows.
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System – локальная политика безопасности.
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer – политика ограничения запуска приложений (наличие там путей к антивирусу может привести к его нерабоспособности).

Раздел обработчика системных типов файлов:

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile – EXE
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\cmdfile – CMD
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\piffile – PIF
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\batfile – BAT
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\comfile – COM
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\scrfile – SCR
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile – LNK

Проанализировать результаты работы Dr.Web SysInfo вы можете самостоятельно, а можете отправить их в службу технической поддержки «Доктор Веб». В первом случае вам понадобится не только материал из нашего пособия, но и, возможно, литература по Windows. При отправке отчета в «Доктор Веб» вам останется только выполнить рекомендации профессионалов.

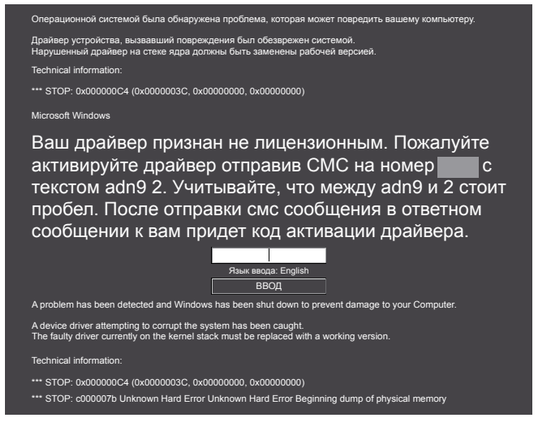
11. Борьба с троянцами семейства WinLock и MbrLock (блокировщики Windows)

11.1. Актуальность вопроса

Троянцы, блокирующие работу Windows, с сентября 2009 года — одни из самых распространенных по частоте проявления. Например, за декабрь 2010 года более 40% обнаруженных вирусов — блокировщики Windows. Общее название подобных вредоносных программ — Trojan.Winlock.XXX, где XXX — номер, присвоенный сигнатуре, которая позволяет определить несколько (зачастую несколько сотен) схожих вирусов. Также подобные программы могут относиться к типам Trojan.Inject или Trojan.Siggen, но такое случается значительно реже.

Внешне троянец может быть двух принципиальных видов. Первый: заставка на весь экран, из-за которой не видно рабочий стол, второй: небольшое окно в центре. Второй вариант не закрывает экран полностью, но баннер все равно делает невозможной полезную работу с ПК, поскольку всегда держится поверх любых других окон.

Вот классический пример внешнего вида программы Trojan.Winlock:



Цель троянца проста: добыть для вирусописателей побольше денег с жертв вирусной атаки.

Наша задача — научиться быстро и без потерь устранять любые баннеры, ничего не платя злоумышленникам. После устранения проблемы необходимо написать заявление в полицию и предоставить сотрудникам правоохранительных органов всю известную вам информацию.

Внимание! В текстах многих блокировщиков встречаются различные угрозы («у вас осталось 2 часа», «осталось 10 попыток ввода кода», «в случае переустановки Windows все данные будут уничтожены» и т. д.). В основном это не более чем блеф.

11.2. Алгоритм действий по борьбе с Trojan.Winlock

Модификаций блокировщиков существует великое множество, но и число известных экземпляров очень велико. В связи с этим лечение зараженного ПК может занять несколько минут в легком случае и несколько часов, если модификация еще не известна. Но в любой ситуации следует придерживаться приведенного ниже алгоритма:

1. Подбор кода разблокировки. Коды разблокировки ко многим троянцам уже известны и занесены в специальную базу, созданную специалистами компании «Доктор Веб». Чтобы воспользоваться базой, перейдите по ссылке *http://www.drweb.com/unlocker/index/?lng=ru* и попробуйте подобрать код. Инструкция по работе с базой разблокировки:

Прежде всего, попробуйте получить код разблокировки, воспользовавшись формой, позволяющей ввести текст сообщения и номер, на который его нужно отправить. Обратите внимание на следующие правила:

- Если требуется перевести деньги на счет или телефонный номер, в поле *Номер* необходимо указать номер счета или телефона, в поле *Текст* ничего писать не нужно.
- Если требуется перевести деньги на телефонный номер, в поле *Номер* необходимо указать номер телефона в формате 8xxxxxxxxxx, даже если в баннере указан номер без цифры 8.
- Если требуется отправить сообщение на короткий номер, в поле *Номер* укажите номер, в поле *Текст* — текст сообщения.

Если сгенерированные коды не подошли — попробуйте вычислить название вируса с помощью представленных картинок. Под каждым изображением блокировщика указано его название. Найдя нужный баннер, запомните название вируса и выберите его в списке известных блокировщиков. Укажите в выпадающем списке имя вируса, поразившего ваш ПК, и скопируйте полученный код в строку баннера.

Обратите внимание, что, кроме кода, может быть выдана другая информация:

- *Win+D to unlock* — нажмите комбинацию клавиш *Windows+D* для разблокировки.
- *any 7 symbols* — введите любые 7 символов.
- *Воспользуйтесь генератором выше* или *use generator above* — используйте для получения кода разблокировки форму *Номер-Текст* в правой части окна.
- *Используйте форму* или *Пожалуйста, воспользуйтесь формой* — используйте для получения кода разблокировки форму *Номер-Текст* в правой части окна.

2. Если система заблокирована частично. Этот шаг относится к случаям, когда баннер «висит» в середине экрана, не занимая его целиком. Если доступ заблокирован полностью — переходите сразу к шагу 3. Диспетчер задач при этом блокируется аналогично полноэкранным версиям троянца, то есть завершить вредоносный процесс обычными средствами нельзя. Пользуясь остатками свободного пространства на экране, сделайте следующее:

1) Проверьте ПК свежей версией лечащей утилиты Dr.Web CureIt! (порядок работы с Dr.Web CureIt! см в разделе 12). Если вирус благополучно удален, дело можно считать сделанным, если ничего не найдено — переходите к шагу 4.
2) Скачайте восстанавливающую утилиту Dr.Web Trojan.Plastix fix по ссылке *http://download.geo.drweb.com/pub/drweb/tools/plstfix.exe* и запустите скачанный файл. В окне программы нажмите *Продолжить*, и когда Plastixfix закончит работу, перезагрузите ПК.
3) Попробуйте установить и запустить программу Process Explorer (скачать можно с сайта Microsoft: *http://technet.microsoft.com/ru-ru/sysinternals/bb896653*). Если запуск удался — нажмите мышью в окне программы кнопку с изображением прицела и, не отпуская ее, наведите курсор на баннер. Когда вы отпустите кнопку, Process Explorer покажет процесс, который отвечает за работу баннера.

3. Если доступа нет совсем. Обычно блокировщики полностью загромождают баннером экран, что делает невозможным запуск любых программ, в том числе и Dr.Web CureIt! В этом случае необходимо загрузиться с Dr.Web LiveCD или Dr.Web LiveUSB и проверить ПК на вирусы (инструкция — в разделе 11). После проверки загрузите компьютер с жесткого диска и проверьте, удалось ли решить проблему. Если нет — переходите к шагу 4.

4. Ручной поиск вируса. Если вы дошли до этого пункта, значит дело плохо — поразивший систему троянец — новинка, и искать его придется вручную. Для работы нам понадобится Dr.Web LiveCD/USB. Загрузите ПК с компакт-диска или флешки, после чего скопируйте на флеш-карту следующие файлы:

- C:\Windows\System32\config\software *файл не имеет расширения*
- C:\Document and Settings\Ваше_имя_пользователя\ntuser.dat

В этих файлах содержится системный реестр зараженной машины. Обработав их в программе *Regedit*, мы сможем очистить реестр от последствий вирусной активности и одновременно найти подозрительные файлы.

Теперь скопируйте указанные файлы на функционирующий ПК под управлением Windows и сделайте следующее:

Запустите Regedit, откройте куст *HKEY_LOCAL_MACHINE* и выполните *Файл –> Загрузить куст*. В открывшемся окне укажите путь к файлу *software*, задайте имя (например, текущую дату) для раздела и нажмите *OK*.

В этом кусте необходимо проверить следующие ветки:

Microsoft\Windows NT\CurrentVersion\Winlogon:

- Параметр Shell должен быть равен Explorer.exe. Если перечислены любые другие файлы — необходимо записать их названия и полный путь к ним. Затем удалить все лишнее и задать значение Explorer.exe.
- Параметр userinit должен быть равен C:\Windows\system32\userinit.exe, (именно так, с запятой на конце, где C — имя системного диска). Если указаны файлы после запятой — нужно записать их названия и удалить все, что указано после первой запятой.

Встречаются ситуации, когда присутствует схожая ветвь с названием *Microsoft\Windows NT\CurrentVersion\winlogon*. Если эта ветвь есть, ее необходимо удалить.

Microsoft\Windows\CurrentVersion\Run — ветвь содержит настройки объектов автозапуска. Особенно внимательно следует отнестись к наличию здесь объектов, отвечающих следующим критериям:

- Имена напоминают системные процессы, но программы запускаются из других папок (например, C:\Documents and Settings\Dima\svchost.exe).
- Имена вроде vip-porno-1923.avi.exe.
- Приложения, запускающиеся из временных папок.
- Неизвестные приложения, запускающиеся из системных папок (например, C:\Windows\system32\install.exe).
- Имена состоят из случайных комбинаций букв и цифр (например, C:\Documents and Settings\Dima\094238387764\094238387764.exe).

Если подозрительные объекты присутствуют — их имена и пути необходимо записать, а соответствующие им записи удалить из автозагрузки.

Microsoft\Windows\CurrentVersion\RunOnce — тоже ветвь автозагрузки, ее необходимо проанализировать аналогичным образом.

Завершив анализ, нажмите на имя загруженного раздела (в нашем случае он называется по дате) и выполните *Файл –> Выгрузить куст*.

Теперь необходимо проанализировать второй файл — NTUSER.DAT. Запустите Regedit, откройте куст *HKEY_LOCAL_MACHINE* и выполните *Файл –> Загрузить куст*. В открывшемся окне укажите путь к файлу *NTUSER.DAT*, задайте имя для раздела и нажмите *OK*.

Здесь интерес представляют ветки *Software\Microsoft\Windows\CurrentVersion\Run* и *Software\Microsoft\Windows\CurrentVersion\RunOnce*, задающие объекты автозагрузки. Необходимо проанализировать их на наличие подозрительных объектов, как указано выше.

Также обратите внимание на параметр Shell в ветке *Software\Microsoft\Windows NT\CurrentVesion\Winlogon*. Он должен иметь значение Explorer.exe. В то же время, если такой ветки нет вообще — все в порядке.

Завершив анализ, нажмите на имя загруженного раздела (в нашем случае он называется по дате) и выполните *Файл –> Выгрузить куст*.

Получив исправленный реестр и список подозрительный файлов, необходимо сделать следующее:

- Сохраните реестр пораженного ПК на случай, если что-то было сделано неправильно.
- Перенесите исправленные файлы реестра в соответствующие папки на пораженном ПК с помощью Dr.Web LiveCD/USB (копировать с заменой файлов).
- Файлы, информацию о которых вы записали в ходе работы — сохраните на флешке и удалите из системы. Их копии необходимо отправить в вирусную лабораторию компании «Доктор Веб» на анализ.

Попробуйте загрузить инфицированную машину с жесткого диска. Если загрузка прошла успешно и баннера нет — проблема решена. Если троянец по-прежнему функционирует, повторите весь пункт 4 этого раздела, но с более тщательным анализом всех уязвимых и часто используемых вирусами мест системы. Подробнее об этом написано в разделе 5.

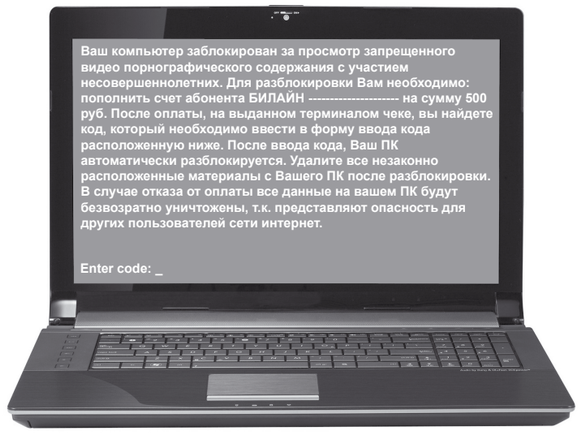
Внимание! Если после лечения с помощью Dr.Web LiveCD/USB компьютер не загружается (начинает циклически перезагружаться, возникает BSOD), нужно сделать следующее:

- Убедитесь, что в папке config находится один файл software. Проблема может возникать, потому что в Unix-системах регистр в имени файлов имеет значение (т. е. Software и software — разные имена, и эти файлы могут находиться в одной папке), и исправленный файл software может добавиться в папку без перезаписи старого. При загрузке Windows, в которой регистр букв роли не играет, происходит конфликт и ОС не загружается. Если файлов два — удалите более старый.
- Если software один, а загрузка не происходит, высока вероятность, что система поражена «особенной» модификацией Winlock. Она прописывает себя в ветку HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, в параметр Shell и перезаписывает файл userinit.exe. Оригинальный userinit.exe хранится в той же папке, но под другим именем (чаще всего 03014d3f.exe). Удалите зараженный userinit.exe и переименуйте соответствующим образом 03014d3f.exe (имя может отличаться, но найти его легко). Эти действия необходимо провести, загрузившись с Dr.Web LiveCD/USB, после чего попробовать загрузиться с жесткого диска.

На каком бы из этапов ни кончилась битва с троянцем, необходимо обезопасить себя от подобных неприятностей в будущем. Установите антивирусный пакет Dr.Web и регулярно обновляйте вирусные базы.

11.3. Алгоритм действий по борьбе с Trojan.Mbrlock

В последнее время появились троянцы семейства Trojan.Mbrlock (*http://vms.drweb.com/virus/?i=589788*), которые внешне не отличаются от Trojan.Winlock, отчего их часто путают, но действуют по совершенно другому принципу. Trojan.Mbrlock перезаписывает главную загрузочную запись (MBR) жесткого диска, и при включении ПК загружает основной вирусный код из следующих за MBR областей. При этом пользователь видит все тот же экран с сообщением о блокировке и информацию о способах оплаты. Чаще всего экран вредоносной программы выглядит так:



Для борьбы с Trojan.Mbrlock проводить какие-либо операции с реестром не требуется — троянец не прописывает себя в ключи реестра, поскольку никак не взаимодействует с ОС, поражая диск на низком уровне. Оптимальным будет провести лечение с помощью последней версии Dr.Web LiveCD/USB — троянец успешно детектируется, и оригинальная MBR восстанавливается.

Стоит отметить, что значительная часть вредоносных программ этого типа запрограммированы на функционирование до определенной даты, после чего оригинальная MBR автоматически восстанавливается. Если лечение не помогло, или недоступна самая новая версия LiveCD, нужно, загрузив ПК с другого жесткого диска или сменного носителя, поменять системную дату на более позднюю — вполне возможно, троянец сам восстановит пораженную MBR.

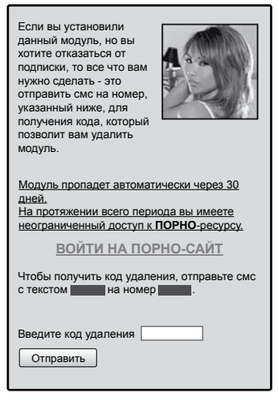
Когда восстановление системы завершено, необходимо отыскать исполняемый файл троянца, чтобы отправить его на анализ. Обычно это файл с расширением .exe, который находится в папке Temp пользовательского профиля. С помощью Dr.Web LiveCD/USB скопируйте все exe-файлы из этой папки и отправьте в антивирусную лабораторию «Доктор Веб». После отправки подозрительных файлов папку лучше всего очистить, чтобы предотвратить повторную активацию вредоносной программы.

Внимание! При поражении системы Torjan.Mbrlock не рекомендуется пользоваться программами, восстанавливающими главную загрузочную запись. Троянец может хранить оригинальный MBR в одном из начальных секторов, и попытка восстановления может не помочь делу, но уничтожить запись оригинального MBR, что сделает невозможным восстановление обычными методами.

12. Борьба с вирусами семейства HTTPBlock и BrowseBan (блокировщики браузеров)

В этом разделе речь пойдет о троянцах, блокирующих работу интернет-обозревателей и сетевых приложений: Trojan.BrowseBan (*http://vms.drweb.com/virus/?i=441472*) и Trojan.HTTPBlock.

Работу вновь начинаем с постановки проблемы: имеется нормально функционирующий ПК с доступом в Интернет. Но попытка открыть какой-либо сайт в любом установленном браузере не дает результата (реже встречаются ситуации, когда в одном браузере все работает, а второй заблокирован). Открывается либо одна и та же веб-страница, либо баннер в пол-окна, например такой:



Этот вариант баннера используется многими вирусами. Наша задача вернуть функционирование браузера в норму, ничего никому не платя.

Ниже приведен общий алгоритм действий. На каком именно шаге вы сможете вернуть доступ в Интернет — будет зависеть от вируса. В любом случае, выполнив весь цикл, вы сделаете только лучше.

1. Проверить и очистить файл HOSTS. Файл HOSTS содержит сопоставления IP-адресов именам узлов и в изначальном состоянии содержит всего одну действующую строку (все остальное — комментарии):

127.0.0.1 localhost

Файл не имеет расширения и располагается в папке C:\WINDOWS\system32\drivers\etc. Как правило, вирусы в первую очередь модифицируют именно HOSTS, прописывая там перенаправление со многих популярных сайтов на локальный компьютер или на вредоносный сервер. Чтобы исправить это, откройте Hosts с помощью программы Блокнот и удалите все строки, кроме указанной выше. Проверьте, удалось ли решить проблему.

Зачастую мошенники применяют различные хитрости, осложняющие задачу по борьбе с вирусом, вот наиболее популярные уловки:

- ***Полоса прокрутки.*** При открытии файл HOSTS выглядит нетронутым, если не обращать внимания на полосу прокрутки справа. Но наличие полосы прокрутки говорит о том, что далеко внизу (может быть 70 или больше пустых строчек) все-таки есть список перенаправления, но при открытии файла в окне сразу увидеть его нельзя. Прокрутите файл до конца и уберите все лишнее.
- ***Подмена пути к файлу.*** Файл HOSTS может оказаться нетронутым, но в то же время ***не обрабатываться Windows!*** Положение базы данных, которую и представляет собой

hosts, задается в реестре ключе *DataBasePath* в ветке \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\. Открыв этот ключ с помощью Regedit, убедитесь, что ключ указывает именно на системную папку (значение ключа должно быть *%SystemRoot%\System32\drivers\etc*), а не на постороннюю. Если значение неверное – замените его правильным и вновь попробуйте открыть какой-либо сайт.

- ***Ложный файл.*** В папку C:\WINDOWS\system32\drivers\etc, кроме файла HOSTS, может быть помещен другой файл со схожим названием. Поскольку Windows обрабатывает путь, то есть все содержимое папки, воспринят будет и настоящий hosts, и файлы, которые помещены туда дополнительно. Чаще всего в указанную папку записываются скрытые файлы с именами hosts2, host или им подобными. Включите отображение скрытых и системных файлов, отображение системных папок, после чего проверьте, есть ли «лишние» файлы, и удалите их.

Примечание. В SpIDer Guard есть возможность защитить hosts от модификации, а при проверке сканером или Dr.Web CureIt! в случае модифицированного файла hosts выдается соответствующее предупреждение, позволяющее вернуть базу данных в начальное состояние.

2. Проверить настройки прокси в браузере. Следующий шаг вируса после модификации файла HOSTS – изменение настроек браузера. Речь идет о такой опции, как "Используемый прокси-сервер». В небольших сетях и на домашних ПК прокси-серверы обычно не используются, поэтому большая часть пользователей даже не знает об их существовании.

Для устранения проблемы с доступом в Интернет необходимо проверить настройки прокси в браузере и, при необходимости, обнулить их:

- ***Internet Explorer.*** Откройте меню *Сервис –> Свойства обозревателя*. На вкладке *Подключения* нажмите *Настройка сети*. В открывшемся окне снимите флажки со всех пунктов и нажмите *OK*.
- ***Opera.*** Нажмите комбинацию клавиш Ctrl+F12. В открывшемся окне перейдите на вкладку *Расширенные*, в левом меню перейдите на *Сеть* и выберите *Прокси-серверы*. Снимите флажки со всех пунктов меню и нажмите *OK*.
- ***Firefox.*** Откройте меню *Инструменты –> Настройки –> Дополнительно*. На вкладке *Сеть* нажмите *Настроить* и в открывшемся окне отметьте флажком пункт *Без прокси*.

Примечание. Если настройки прокси в вашем браузере подверглись изменению, запишите на лист бумаги адрес прокси-сервера, в дальнейшем он нам понадобится. Например, там может быть адрес 77.78.240.31.

3. Удалить из реестра созданные вирусом ключи. В предыдущем шаге мы получили адрес прокси-сервера, на который производил перенаправление вирус. Чтобы блокировка не повторилась, необходимо убрать из реестра все ключи с этим адресом. Запустите Regedit и с помощью клавиш Ctrl+F (Найти) и F3 (Найти далее) удалите все ключи реестра, где встречается найденный вами адрес, в нашем примере это 77.78.240.31. Также, если был обнаружен вредоносный процесс, нужно удалить все ключи, содержащие его имя.

Если вы подозреваете, что какой-то ключ нельзя удалять, достаточно просто удалить присвоенное ему значение.

5. Проверить специфические варианты работы вируса. К этому пункту относится работа по устранению нескольких известных вирусных действий для конкретных браузеров:

- ***Internet Explorer.*** В стандартном браузере от Microsoft наиболее уязвимую часть составляют BHO (англ. Browser Helper Object – вспомогательные объекты браузера). BHO – это плагины для Internet Explorer, которые могут быть как полезными для пользователя (если созданы легальными компаниями), так и вредоносными. Чтобы отключить обработку плагинов, в

главном меню браузера нажмите *Сервис –> Надстройки* и в открывшемся окне отключите ненужные надстройки с помощью кнопки *Отключить*.

- ***Opera.*** Часто баннер устанавливается пользовательским скриптом. Чтобы избавить от него, достаточно удалить папку пользовательских скриптов. Ее расположение можно посмотреть в настройках браузера: нажмите комбинацию клавиш Ctrl+F12, перейдите на вкладку *Расширенные*, в левом меню нажмите *Содержимое* и выберите *Настроить JavaScript*. В строке открывшегося окна указана папка, где содержатся пользовательские скрипты. Откройте ее через *Проводник* и удалите все файлы.
- ***Firefox.*** Здесь баннеры запускаются из пользовательских дополнений. Чтобы удалить его, придется пожертвовать всеми дополнениями, если вам точно не известно название вируса (так обычно и бывает). Пользовательские дополнения хранятся в папке C:\Program Files\Mozilla Firefox\extensions.

6. Провести полную антивирусную проверку компьютера. Даже если проблема была решена на первом или втором шаге, но вирус, ставший ее причиной, сохранился на ПК, рано или поздно ситуация повторится. Чтобы этого избежать, необходимо установить антивирус, например от компании «Доктор Веб» (*www.drweb.com*). После установки обновите базы и проверьте ПК на вирусы.

Если антивирус другого производителя уже установлен, воспользуйтесь антивирусной утилитой Dr.Web CureIt! (*www.freedrweb.com*), позволяющей проверить компьютер даже при наличии другого антивируса.

Все подозрительные объекты, найденные антивирусом, необходимо отправлять в лабораторию «Доктор Веб» с помощью сайта: *https://vms.drweb.com/sendvirus/?lng=ru*.

12.1. Алгоритм действий при вирусном изменении домашней страницы

Действия троянцев из семейства Trojan.Starter (*http://vms.drweb.com/virus/?i=9284*) не имеют прямого отношения к главным «героям» этого раздела, зато, подобно им, проявляют свою активность в браузерах. Первый и единственный признак поражения компьютера Trojan.Starter – это изменение домашней страницы на нежелательную без участия пользователя. В браузере Opera зачастую меняется стартовый внешний вид – вместо экспресс-панели открывается установленный троянцем сайт.

Важно, что при поражении этим троянцем восстановить стартовую страницу через стандартные настройки браузера невозможно – после перезагрузки браузера или ПК проблема возникает вновь.

Чаще всего в качестве стартовых страниц устанавливаются следующие ресурсы (**не переходите по ссылкам!**):

- www.webalta.ru
- www.apeha.ru
- www.ctel.ru
- www.smaxi.net
- www.wonderpage.org

Путь к решению проблемы варьируется в зависимости от используемого браузера. Общими являются лишь два момента:

- Все действия необходимо выполнять при закрытом браузере, кроме тех пунктов, где нужно работать непосредственно в нем.
- После работы с файлами и папками любого браузера обязательно проведите чистку реестра (см. пункт про Internet Explorer).

Internet Explorer

- Нажмите *Пуск –> Выполнить*, введите *regedit* и нажмите *OK*.
- В меню реестра выберите *Правка –> Найти*, в строке поиска напечатайте название сайта, заменившего вашу домашнюю страницу (например: *webalta*), и нажмите *OK*.
- Найдя первую запись с таким значением, необходимо очистить ее, удалив значение записи. Удалять саму запись нельзя!
- Нажмите F3 для поиска следующей записи с искомым словом. Очистите ее и переходите к следующей. Поиск нужно провести до конца реестра.
- Когда работа завершена, закройте редактор реестра.
- Откройте Internet Explorer и установите нужную вам домашнюю страницу в его настройках.

Opera

Откройте папку C:\Windows\system32 (где C: – диск установки ОС) и найдите в ней файл *operaprefs_fixed.ini*. Просматривая его, вы, вероятно, обнаружите код, изменяющий домашнюю страницу. Например, в случае с webalta.ru код выглядит следующим образом:

[User Prefs]
Home URL=http://webalta.ru
Startup Type=2

Если такой или ему подобный код присутствует в файле – удалите его и закройте файл, сохранив изменения. После этого можно запустить Opera и задать прежнюю домашнюю страницу или режим экспресс-панели.

Firefox

Если проблема связана со страницей webalta.ru, в Firefox откройте меню *Справка –> Информация для решения проблем*, после чего в открывшемся окне нажмите кнопку *Открыть его папку*. Откроется папка с профилем Firefox. В ней необходимо найти два файла – user.js и prefs.js. Просмотрите их в любом текстовом редакторе, например Блокноте. Код, изменяющий стартовую страницу, выглядит так:

user_pref("startup.homepage_override_url", "http://webalta.ru");
user_pref("browser.startup.page", 1);
user_pref("browser.startup.homepage", "http://webalta.ru");

Если код обнаружен и при этом файл *user.js*, не содержит других записей, его нужно удалить. *Prefs.js* удалять нельзя, достаточно убрать из него строки, влияющие на изменение домашней страницы.

Если проблема связана с любой другой страницей, наберите в адресной строке браузера *about:config* и нажмите *Enter*. В появившемся предупреждении выберите *Я обещаю, что буду осторожен*.

Откроется реестр Firefox. Введите в строку поиска название установленной троянцем домашней страницы (apeha.ru, wonderpage.org и др.), и реестр выведет перечень записей, содержащих упоминание о ней. Очистите значения этих записей и перезапустите браузер.

13. Борьба с вирусами семейства Trojan.Encoder (вирусы-шифровальщики)

Троянцы семейства Trojan.Encoder (*http://vms.drweb.com/virus/?i=472*) – один из самых неприятных типов вредоносного ПО. Активировавшись в системе, они шифруют содержащиеся на диске файлы, делая их содержимое недоступным для приложений и самого пользователя. Шифрование может производиться по нескольким алгоритмам, чаще всего XOR (метод шифрования, основанный на операции «исключающее ИЛИ» – eXclusive OR) и различные модификации TEA (Tiny Encryption Algorithm, блочный алгоритм шифрования). Шифровке подвергаются файлы наиболее распространенных типов: .rtf, .txt, .pdf, .xls, .rar, .zip, .xml, .c, .cpp, .h, .pgp, .jpg .jpeg, .psd, .mov, .doc, .docx, .xlsx, .ppt, .pptx, .db, .mdb, .dbf, .php, .mp3 и многие другие. Исполняемые файлы программ, как правило, не шифруются, но сами приложения становятся бесполезными, поскольку все обрабатываемые ими файлы делаются недоступными.

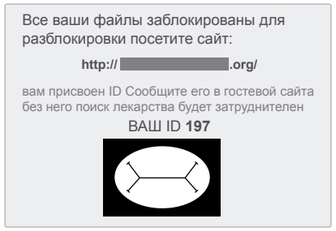
Этот вид вредоносного ПО обычно распространяется через электронную почту и Интернет, могут использовать уязвимости браузеров.

К вопросам восстановления данных после атаки Trojan.Encoder нужно подходить очень осторожно, поскольку неверные действия могут привести к потере зашифрованных данных.

Постановка проблемы: имеется компьютер, рабочие файлы которого зашифрованы троянцем. Наша задача восстановить всю информацию, после чего удалить вредоносное ПО из системы. Для достижения цели необходимо будет выполнить следующие шаги:

Шаг 1. Необходимо определить, какой именно модификацией Trojan.Encoder поражена система. Основные модификации шифровальщиков отличаются следующими признаками:

- **К зашифрованным файлам добавилось одно из расширений: .icq550946977, .pizdec, .GpCODE, .a.** Указывает на вирус Trojan.Encoder.94.
- **К зашифрованным файлам добавилось одно из расширений: .korrektor, .exe, .bloc, .gggg, .diablo, .cool, .vhd, .mmm, .kis, .mis, .web.** Любое из них могут иметь файлы, зашифрованные Trojan.Encoder.71.
- **К зашифрованным файлам добавилось расширение .Crypted.** Результат деятельности Trojan.Encoder.91.
- **К зашифрованным файлам добавилось расширение .Encrypted.** Оно присваивается файлам при шифровании троянцами Trojan.Encoder.94 и Trojan.Encoder.99.
- **Файлы сжаты в ZIP-архивы, защищенные паролем.** Это специфика Trojan.Encoder.68.
- **Расширение файлов не меняется, на рабочем столе появляется сообщение с требованием оплаты и данными для платежа. Также в конец зашифрованных файлов добавились строки вида: "B3E36CB6475B5EB08D9507E09A0978880C28E1E3F6497B93C945738DB5D7B31DC2BDBFDF14E797DC".** Этим отличается Trojan.Encoder.102.
- **Расширение файлов не изменилось, но на рабочем столе появилось сообщение, аналогичное приведенному на рисунке ниже:**



Здесь важно обратить внимание на ID и запомнить его. Подобным образом файлы шифрует Trojan.Encoder.96.

Шаг 2. Исходя из названия троянской программы, можно подобрать соответствующую утилиту для дешифровки. Компанией «Доктор Веб» выпущены бесплатные утилиты для восстановления файлов после поражения системы вирусами-шифровальщиками. Утилиты можно скачать по ссылке: *ftp://ftp.drweb.com/pub/drweb/tools*. Описанным выше шифровщикам соответствуют следующие утилиты:

- Trojan.Encoder.94/Trojan.Encoder.99 — *ftp://ftp.drweb.com/pub/drweb/tools/te94decrypt.exe*
- Trojan.Encoder.71/Trojan.Encoder.96 — *ftp://ftp.drweb.com/pub/drweb/tools/te71decrypt.exe*
- Trojan.Encoder.91 — *ftp://ftp.drweb.com/pub/drweb/tools/te91decrypt.exe*
- Trojan.Encoder.102 — *ftp://ftp.drweb.com/pub/drweb/tools/te102decrypt.exe*
- Trojan.Encoder.68 — для получения пароля воспользуйтесь ссылкой: *http://www.freedrweb.com/aid_admin/decode+encoder*. В поле необходимо ввести ID, указанный в файлах Readme.txt, которые создаются в папках с зашифрованными файлами.

Всегда используйте наиболее новые версии утилит дешифровки, скачивая их с нашего сайта. Например, актуальной версией сейчас являются 1.3.9 для 94-й утилиты и 1.4.15 для 71-й.

Шаг 3. Скачав соответствующую утилиту, можно приступать к расшифровке файлов. Ниже приведен алгоритм работы со всеми упомянутыми утилитами:

- ***Te94decrypt.exe.*** Для дешифровки файлов от Trojan.Cncoder94/99 сперва необходимо подобрать подходящий ключ расшифровки. Для подбора ключа необходимо сделать следующее:

1. Скопируйте дешифровщик te94decrypt.exe в корневую папку диска C: и запустите его через меню *Пуск –> Выполнить*. В строке запуска введите без кавычек: *"C:\te94decrypt.exe любой_файл"*. Утилита автоматически расшифрует файл по всем возможным вариантам декодирования.
2. Будет создано несколько (иногда более 10) копий расшифрованного файла, название каждой из которых будет оканчиваться набором символов "-kN", где N — некоторое число. Например, один из вариантов расшифрованного файла может называться *archive.rar-k201*. Число 201 — один из вариантов ключа.
3. Откройте поочередно все расшифрованные файлы и найдите тот, который расшифрован правильно. Обратите внимания, какой ключ соответствует верному декодированию.
4. Запустите утилиту дешифровки Пуск, вместо имени файла указав подобранный ключ (например: *C:\te94decrypt.exe –k 201*).

- ***Te91decrypt.exe.*** Для дешифровки всех файлов достаточно запустить утилиту двойным щелчком мыши и в открывшемся окне нажать Продолжить.
- ***Te102decrypt.exe.*** Для дешифровки всех файлов достаточно запустить утилиту двойным щелчком мыши и в открывшемся окне нажать Продолжить.
- ***Te71decrypt.exe.*** Работа с этой утилитой разнится в зависимости от модификации вируса, зашифровавшего файлы:
- ***Trojan.Encoder.71.*** Для расшифровки файлов запустите утилиту двойным щелчком мыши и нажмите *Продолжить*.
- ***Trojan.Encoder.96.*** Скопируйте дешифровщик te71decrypt.exe в корень диска C: и запустите его через меню *Пуск –> Выполнить*. В строке запуска введите без кавычек: "*C:\te71decrypt.exe –k ID*", где ID — цифры, указанные на измененных вирусом обоях рабочего стола (в нашем примере 197).

Шаг 4. Проверьте расшифрованные файлы в нескольких папках. Если все в порядке, значит, декодирование выполнено успешно, и можно приступать к последнему этапу — уничтожению файла троянца.

Для этого можно использовать либо антивирус (предварительно обновив базы), либо утилиту Dr.Web CureIt! (см. раздел 12).

Примечание. До того как файлы расшифрованы, в системе нельзя производить никаких действий! В их число входят:

- Проверка и лечение компьютера с помощью антивируса или утилиты Dr.Web CureIt! (или аналогичной).
- Переустановка Windows.
- Перемещение или удаление ***любых*** (в том числе не зашифрованных) файлов на компьютере.
- Если на компьютере (в корне диска C:\ или папке профиля пользователя) появились файлы с названиями crypted, pass или другими подобными — ***их ни в коем случае нельзя перемещать или удалять!***
- ***Очистка истории браузера.***

Примечание. Проверять, правильно расшифрованы файлы или нет, проще всего с помощью архивов. Для этого достаточно открыть любой декодированный архив и провести* Проверку целостности *или* Тест архива *(зависит от используемого архиватора).

Приложение 1. Типы вредоносного ПО

Вредоносное программное обеспечение — общий термин, включающий в себя множество подвидов программ, которые могут нарушить работу компьютера, повредить информацию или нанести другой вид ущерба. В этом разделе мы ознакомимся со всеми видами вредоносного ПО.

Вирусы

Компьютерные вирусы отличаются от прочих программ способностью к самовоспроизведению. Ключевые термины в данном разделе:

Вирусный код, сигнатура (Signature) — система символов и однозначных правил их интерпретации, используемая для предоставления информации. Это набор символов или последовательность байтов, которые могут быть свойственны какому-либо определенному вирусу (и только ему), в частности, каждой его копии. Антивирусные сканеры используют сигнатуры для нахождения вирусов.

Дроппер (Dropper) — файл-носитель, устанавливающий вирус в систему. Техника, иногда используемая вирусописателями для «прикрытия» вирусов от антивирусных программ.

Вариант вируса, штамм, модификация (Variant, modification) — модифицированный вариант одного и того же вируса. Изменения в код могут вноситься как самим автором вируса, так и посторонними.

Компьютерные вирусы (Computer viruses) — это программы или фрагменты программного кода, которые, попав на компьютер, могут вопреки воле пользователя выполнять различные операции на зараженном ПК — создавать или удалять объекты, модифицировать файлы данных или программ, осуществлять действия по собственному распространению по локальным вычислительным сетям или Интернету. Модификация данных происходит таким образом, что зараженные объекты становятся носителями вирусного кода и, в свою очередь, могут осуществлять вышеперечисленные операции. Способность к самовоспроизведению — это важнейшая отличительная черта компьютерных вирусов.

Основными типами вирусов являются:

Анти-антивирусный вирус (Anti-antivirus Virus, Retrovirus) — компьютерная вирусная программа, объектом нападения которой являются антивирусы.

Вирусная программа-червь (Worm-virus) — паразитическая программа, обладающая механизмом саморазмножения. Программа способна размножать свои копии, но не поражать другие компьютерные программы. Проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через Интернет) и рассылает свои функциональные копии на другие ПК сети.

Распространяются черви по двум основным каналам: через уязвимости в системах безопасности установленного ПО и методами социальной инженерии (в этом они схожи и с прочим вредоносным ПО).

Область «деятельности» червей может различаться — некоторые представители этого вида просто распространяются по сетям, не причиняя никакого вреда, кроме забитых каналов, другие могут вредить информации и воровать пароли, третьи устанавливают в систему другие типы вредоносных программ.

Подробнее о сетевых червях можно прочитать по ссылке: *http://ru.wikipedia.org/wiki/Сетевые_черви*.

Вирусы-спутники, вирусы-компаньоны (Virus-companion) — формально являются файловыми вирусами. Не внедряются в исполняемые программы.

Такие вирусы используют особенность системы DOS, позволяющую программному файлу с тем же названием, но другим расширением действовать с разными приоритетами.

Под приоритетом понимают присваиваемый задачам, программам или операциям признак, определяющий очередность их выполнения вычислительной системой.

Большинство таких вирусов создают COM-файл, который обладает более высоким приоритетом, нежели EXE-файлы с тем же названием. При запуске файла по имени (без указания расширения) будет запущен файл с расширением .COM.

Такие вирусы могут быть резидентными и маскировать файлы-двойники.

Зоологический вирус (Zoo virus) — вирус, существующий только в антивирусных лабораториях, в коллекция исследователей вирусов и не встречающийся в работающих сетях.

MtE вирусы (MtE viruses) — полиморфные вирусы, созданные с помощью генератора полиморфизма MtE (Mutant Engine). Такой генератор представляет собой специальный алгоритм, который отвечает за функции шифровки/расшифровки и генерацию расшифровщиков, он присоединяется к любому объектному коду вируса. Такой расшифровщик не имеет ни одного постоянного бита, длина его всегда разная.

Стелс-вирусы (Stealth virus) — вирусные программы, предпринимающие специальные действия для маскировки своей деятельности.

Так называемая стелс-технология может включать в себя:

- затруднение обнаружения вируса в оперативной памяти
- затруднение трассировки и дизассемблирования вируса
- маскировку процесса заражения
- затруднение обнаружения вируса в зараженной программе и загрузочном секторе.

Резидентный (находящийся в памяти) вирус (Memory resident virus) — постоянно присутствующий в памяти вирус, написанный, как правило, на языке Ассемблер или C.

Такие вирусы обладают возможностью более эффективно заражать программы и противодействовать антивирусным средствам. Занимая малые объемы оперативной памяти, такой вирус пребывает в состоянии готовности к продолжению выполнения своей задачи до выгрузки, перезагрузки или выключения компьютера. Активизируется и выполняет заданные вирусописателем действия при соблюдении определенного условия, например при достижении компьютером определенного состояния (срабатывание таймера, др.). Все загрузочные вирусы резидентны.

Полиморфные вирусы (Polymorphic viruses) — или вирусы с самомодифицирующимися расшифровщиками (по Н. Н. Безрукову) — вирусы, использующие, помимо шифрования кода, специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у него байтовых сигнатур. Расшифровщик не является постоянным — он уникален для каждого экземпляра вируса.

Скрипт-вирусы (Script virus) — вирусы, написанные на языках Visual Basic, Basic Script, Java Script, Jscript. На компьютер пользователя такие вирусы, чаще всего, проникают в виде почтовых сообщений, содержащих во вложениях файлы-сценарии. Программы на языках Visual Basic и Java Script могут располагаться как в отдельных файлах, так и встраиваться в HTML-документ и в таком виде интерпретироваться браузером, причем не только с удаленного сервера, но и с локального диска.

Шифрованные вирусы (Encrypted viruses) — вирусы, которые сами шифруют свой код для затруднения их дизассемблирования и обнаружения в файле, памяти или секторе. Каждый экземпляр такого вируса будет содержать только короткий общий фрагмент — процедуру расшифровки, который и выбирается в качестве сигнатуры. В случае каждого инфицирования он автоматически зашифровывает себя, каждый раз по-разному. Таким способом вирус пытается избежать обнаружения антивирусными программами.

Другие названия вируса (Other virus names) — антивирусные компании, как правило, дают разные названия одним и тем же вирусам, исходя из собственных правил формирования вирусного имени. В большинстве случаев основное имя вируса (например, Klez, Badtrans, Nimda) одинаково и присутствует в наименовании этого вируса, независимо от антивирусной компании. Различаются в основном префиксы и суффиксы имени вируса, правила использования которых у каждой компании могут быть свои. Например, в классификации вирусов, принятой в компании «Доктор Веб», версии одного и того же вируса нумеруются числами, начиная с 1, в компании Symantec для этих же целей используются заглавные буквы английского алфавита.

Технология ActiveX — технология модификации элементов OCX для создания мультимедийных клиент-серверных приложений, разработанная корпорацией Microsoft. Активно используется злоумышленниками благодаря наличию в ней многочисленных уязвимостей, помогающих проникать на компьютер-жертву.

В зависимости от видов заражаемых объектов, компьютерные вирусы классифицируют по следующим типам:

Файловые вирусы (File viruses) — вирусы, заражающие двоичные файлы (в основном исполняемые файлы и динамические библиотеки). Чаще всего поражают файлы с расширениями .EXE, .COM, .DLL, .SYS, .DRV, .BIN, .OVL и .OVY. Такие вирусы внедряются в файлы операционной системы, активируются при запуске пораженной программы и затем распространяются.

Загрузочные вирусы (буткиты) (Boot viruses) — вирусы, которые заражают загрузочные записи (Boot record) дискет, разделов жестких дисков, а также MBR (Master Boot Record) жестких дисков.

Макрокомандные вирусы (макровирусы) (Macroviruses) — вирусы, заражающие файлы, созданные приложениями Microsoft Office и другими программами, допускающими наличие макрокоманд (чаще всего на языке Visual Basic). Благоприятным фактором распространения вируса служит то, что все основные компоненты Microsoft Office могут содержать встроенные программы (макросы) на полнофункциональном языке программирования, а в Microsoft Word эти макросы автоматически запускаются при открытии любого документа, его закрытии, сохранении и т. д.

Кроме того, имеется общий шаблон NORMAL.DOT и макросы, помещенные в него, автоматически запускаются при открытии любого документа. Учитывая, что копирование макросов из документа в документ (в частности, в общий шаблон) выполняется всего одной командой, среда Microsoft Word идеальна для существования макрокомандных вирусов.

Вирусы, поражающие документы PDF (PDF-exploit) — вирусы, встраивающие себя в PDF-документы за счет известных уязвимостей данного формата. При открытии зараженного файла вирус активизируется и либо сам совершает несанкционированные действия в системе, либо скачивает из сети другой вирус и активизирует его.

Люки (Backdoors) — программы, обеспечивающие вход в систему или получение привилегированной функции (режима работы) в обход существующей системы полномочий. Часто используются для обхода существующей системы безопасности. Люки не инфицируют файлы, но прописывают себя в реестр, модифицируя его ключи.

Руткит (Rootkit) — вредоносная программа, предназначенная для перехвата системных функций операционной системы (API) с целью сокрытия своего присутствия в системе.

Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткиты распространяются либо как самостоятельные программы, либо как дополнение к иным вредоносных программ — люкам, почтовым червям и прочему.

По принципу своей работы руткиты условно разделяют на две группы: User Mode Rootkits (UMR) — работающие в режиме пользователя, и Kernel Mode Rootkit (KMR) — работающие в режиме ядра.

Работа UMR базируется на перехвате функций библиотек пользовательского режима, а работа KMR — на установке в систему драйвера, который осуществляет перехват функций на уровне системного ядра, что значительно усложняет его обнаружение и обезвреживание.

Теперь рассмотрим классификацию компьютерных вирусов в таком виде, в каком их определяет Антивирус Dr.Web.

"HLL." (High Level Language) вирусы

Вирусы, написанные на языках программирования высокого уровня, таких как C, C++, Pascal, Basic и других. В некоторых случаях вирусный код скомпилированных HLL-вирусов сжимают с использованием различных утилит уплотнения (PKLITE, LZEXE, DIET и других).

В группе HLL-вирусов выделяют несколько классов:

"HLLC." (High Level Language Companion) — вирус-компаньон, написанный на языке программирования высокого уровня. Он использует алгоритм инфицирования, который базируется на манипулировании именами файлов в файловой системе. Обычно HLLC-вирус переименовывает оригиналы исполняемых файлов (или перемещает их в другие папки), а затем использует эти названия для создания на их месте вирусной копии.

"HLLO." (High Level Language Overwriting) — перезаписывающий вирус, написанный на языке программирования высокого уровня. HLLO-вирус перезаписывает файл-жертву.

"HLLP." (High Level Language Parasitic) — паразитический вирус, написанный на языке программирования высокого уровня. HLLP-вирус поражает исполняемые файлы, не повреждая их данные.

"HLLW." (High Level Language Worm) — вирусная программа-червь, написанная на языке программирования высокого уровня. Для распространения эти вирусы не нуждаются в хост-файле, а копируют себя в системные папки.

"HLLM." (High Level Language MassMailing Worm) — вирусные программы-черви массовой рассылки, написанные на языке программирования высокого уровня.

Макровирусы для MS Office

Эти вирусы используют особенности форматов файлов и встроенные макроязыки приложений MS Office. В среде Office 2007 на данный момент вирусов не обнаружено, но в 2003 и 2000 они встречаются. Учитывая, что их активность относительно мала, все их можно отнести к редко встречающимся.

"WM." — инфицированию подвергаются документы и шаблоны MS Word 6.0–7.0.

"XM." — инфицированию подвергаются документы MS Excel 5.0–7.0.

"W97M." — инфицированию подвергаются документы и шаблоны MS Word 8.0–9.0 (MS Office'97/2000).

"X97M." — инфицированию подвергаются документы MS Excel 8.0–9.0 (MS Office'97/2000).

"A97M." — инфицированию подвергаются базы данных MS Access'97/2000.

"O97M." — мультиплатформенные макровирусы, инфицированию которыми подвергаются одновременно несколько приложений MS Office.

Троянцы

Вредоносные программы, содержащие скрытый модуль, осуществляющий несанкционированные пользователем действия в компьютере. Эти действия не обязательно будут разрушительными, но они всегда направлены во вред пользователю. Название этого типа атак

происходит от известной легенды о деревянной статуе коня, использованной греками для проникновения в Трою.

Троянские программы-вандалы подменяют какую-либо из часто запускаемых программ, выполняют ее функции или имитируют такое исполнение, одновременно производя вредоносные действия (стирают файлы, разрушают папки, форматируют диски, отсылают мошенникам пароли или другую конфиденциальную информацию, хранящуюся на ПК). Некоторые троянские программы содержат механизм обновления своих компонентов через Интернет.

Trojan — общее название для различных троянцев, которые, в зависимости от характеристик, могут иметь следующие суффиксы:

".PWS" — ворует пароли.

".Backdoor" — вирусная троянская программа, которая содержит в себе RAT-функцию (RAT — Remote Administration Tool — утилита удаленного администрирования).

".Winlock" — троянская программа, блокирующая работу Windows и вместо этого выводящая на экран сообщение (как правило, с требованием денег).

".Hosts" — эти троянцы перенаправляют пользователей с запрошенных страниц на вредоносный сервер в Интернете, атаки с их помощью называются фармингом.

".Starter" — устанавливает определенную интернет-страницу в качестве домашней.

".HttpBlock" — троянец, устанавливающий локальный веб-сервер на зараженном компьютере и перенаправляющий браузер на страницы, которые показывает этот сервер.

".BrowseBan" — выводит в окне браузера баннер, загораживающий всю информацию.

".Downloader" — троянец, скрытно от пользователя загружающий различные вредоносные файлы из Интернета.

".FakeAlert" — имитирует антивирусную или антишпионскую программу с ложным сообщением о найденных угрозах.

".Encoder" — шифрует файлы на жестком диске.

".Inject" — встраиваются («инжектятся») в системные процессы.

".Siggen" — многокомпонентные троянцы, состоят из нескольких модулей.

".MulDrop" — троянец, скрытно от пользователя загружающий различные вирусы, содержащиеся непосредственно в его теле.

".Proxy" — троянец, позволяющий злоумышленнику анонимно работать в Интернете через зараженный компьютер.

".StartPage" (синоним: Seeker) — троянец, несанкционированно подменяющий адрес страницы, указанной в настройках браузера в качестве домашней (стартовой).

".Click" — троянец, организующий перенаправление пользовательских запросов браузеру на определенный сайт.

".KeyLogger" — троянец-шпион; отслеживает и записывает нажатия клавиш на клавиатуре; может периодически пересылать собранные данные злоумышленнику.

".AVKill" — останавливает работу программ антивирусной защиты, сетевые экраны и т. п.; также может удалять эти программы с диска.

".KillFiles", ".KillDisk", ".DiskEraser" — удаляют некоторое множество файлов (файлы в определенных папках, файлы по маске, все файлы на диске и т. п.).

".DelWin" — удаляет необходимые для работы Windows файлы.

".FormatC" — форматирует диск C:, синоним: FormatAll — форматирует несколько или все диски.

".KillMBR" — портит или стирает содержимое главного загрузочного сектора (MBR).

".KillCMOS" — портит или стирает содержимое CMOS.

Скрипт-вирусы

Такие вирусы пишутся на различных языках сценариев. Как правило, это VBS-, JS- и WScript-вирусные программы-черви, которые распространяются через электронную почту.

"VBS." — вирусы, написанные на языке Visual Basic Script.

"JS." — вирусы, написанные на языке Java Script language.

"WScript." — VBS- и/или JS- черви, обычно встроены в HTML-файлы.

"BAT." — вирусы, написанные на языке командного интерпретатора MS-DOS.

Silly-вирусы

Вирусы, которые не обладают никакими особенными характеристиками (такими как текстовые строки, специальные эффекты и т. д.), вследствие чего нет возможности присвоить таким вирусам особенные названия.

"SillyC." — нерезидентные вирусы, объектами поражения которых являются только COM-файлы.

"SillyE." — нерезидентные вирусы, объектами поражения которых являются только EXE-файлы.

"SillyCE." — нерезидентные вирусы, объектами поражения которых являются только COM- и EXE-файлы.

"SillyRC." — резидентные вирусы, объектами поражения которых являются только COM-файлы.

"SillyRE." — резидентные вирусы, объектами поражения которых являются только EXE-файлы.

"SillyRCE." — резидентные вирусы, объектами поражения которых являются только COM- и EXE-файлы.

"SillyO." — нерезидентные вирусы, которые перезаписывают файлы.

"SillyOR." — резидентные вирусы, которые перезаписывают файлы.

Прочие обозначения

"IRC." — вирусные программы-черви, которые распространяются, используя среду Internet Relayed Chat channels.

Также при именовании вирусов компания «Доктор Веб» использует следующие суффиксы:

".generator" — так называемый «Вирусный конструктор».

".based" — суффикс означает, что вирус был сгенерирован специальной программой «Вирусный конструктор» или как модификация какого-то другого, базового (basic) вирусного кода.

".dropper" — общее название для инсталлятора вируса, самого по себе не являющегося вирусом. При запуске инсталлирует вирус в операционную систему (в исполняемый файл, документ, загрузочный сектор и т. д.).

".origin" — вирус, определяемый только с помощью технологии Origins Tracing («Технология поиска похожести»).

Вирусы, поражающие различные операционные системы:

"Win." — поражает 16-битовые исполняемые программы (NE) в операционной системе Windows. NE — NewExe — формат исполняемых файлов операционной системы Windows 3.xx. Некоторые из этих вирусов могут работать не только в среде Windows 3.xx, но также и в Win'95/98/NT.

"Win95." — поражает 32-битовые исполняемые программы (PE и LE(VxD) операционных систем Windows 95/98.

"WinNT." — поражает 32-битовые исполняемые программы (PE) операционной системы Windows NT

"Win32." — поражает 32-битовые исполняемые программы (PE) операционных систем Windows 95/98/NT.

"OS2." — поражают исполняемые программы (LX) операционной системы OS/2.

"Linux." — поражают исполняемые программы операционной системы Linux.

"Java." — вирусы, написанные на языке программирования Java.

"SunOS." — вирусы, работающие в среде ОС SunOS (Solaris).

"Symbian." — вирусы, работающие в среде Symbian OS (мобильная ОС).

"Android." — работают в среде Android на мобильных устройствах.

"WinCE." — работают в среде Windows Mobile на мобильных устройствах.

Нежелательные программы

К этому типу относится вредоносное ПО, не наносящее вреда информации или процессу работы, но отвлекающее пользователя или собирающее персональную информацию о нем. Эти программы в классификации Dr.Web имеют префикс **Program**.

Дозвонщики (Dialers) — специальные компьютерные программы, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон жертве или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам. Сейчас этот метод чаще всего используется с USB-модемами.

Утилиты удаленного администрирования — невредоносные программы, которые могут использоваться во вредоносных целях. Позволяют осуществлять доступ в локальную сеть и проводить в ней действия из любой точки сети Интернет.

Вредоносные программы

К ним относятся программы, не способные к самовоспроизведению, но наносящие вред информации. Все они имеют префикс ***Tools***.

Шпионские модули-роботы (spybots) — не являющиеся вирусами программы, самостоятельные функциональные модули, автономно решающие ту или иную задачу. Используются хакерами для слежения за жизнедеятельностью сети.

Шпионское ПО (spyware) — опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне — создателю или заказчику такой программы. Среди пользователей шпионского ПО — спамеры, рекламщики, маркетинговые агентства, скам-агентства (занимаются брачными аферами), преступные группировки, деятели промышленного шпионажа. Шпионские программы собирают системные

данные, тип браузера, посещаемые веб-узлы, иногда и содержимое файлов на жестком диске жертвы. Такие программы тайно закачиваются на компьютер вместе с каким-либо ПО (чаще всего пиратским) или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон, после чего устанавливаются скрыто от пользователя. Побочные эффекты от присутствия шпионского ПО на компьютере — нестабильная работа браузера и замедление производительности системы.

Клавиатурные перехватчики (Keyloggers) — программы, чьей основной функцией является перехват данных, вводимых пользователем через клавиатуру. Объектами похищения являются персональные и сетевые пароли доступа, логины, данные кредитных карт и другая персональная информация. Зачастую устанавливаются злоумышленниками на ПК пользователя вручную.

Бомбы с часовыми механизмами (Time bombs) — одна из разновидностей логических бомб, в которых срабатывание скрытого модуля определяется временем.

Логические бомбы (Logic bombs) — скрытые модули, встроенные в ранее разработанную и широко используемую программу. Являются средством компьютерного саботажа. Такой модуль является безвредным до определенного события, при наступлении которого он срабатывает (нажатие пользователем определенных кнопок клавиатуры, изменение в файле или наступление определенной даты или времени).

Зомби (Zombies) — маленькие компьютерные программы, разносимые по Интернету компьютерными червями. Программы-зомби устанавливают себя в пораженной системе и ждут дальнейших команд к действию.

Уязвимости

Часть программного кода, позволяющая использовать его для нарушения работы системы и проникновения в локальную сеть. Сегодня прогресс скорости применения уязвимостей достиг таких высот, что временной интервал между публикацией данных об обнаружении «дыры» и изобретением злоумышленниками средств проникновения в систему через такую уязвимость исчисляется всего несколькими днями. Особенно популярны у хакеров и вирусописателей многочисленные уязвимости ПО корпорации Microsoft. Угрозы, относящиеся к этому классу, имеют префикс ***Exploit***. ***Возможные суффиксы***:

".Rtf" — использование уязвимостей в RTF-файлах.
".Pdf" — использование уязвимостей в PDF-файлах.

Прочие угрозы

Здесь мы опишем виды сетевых атак. Иногда они проводятся даже без специальных программ, а если стороннее ПО все же требуется, то оно используется хакерами для нанесения вреда пользователям атакуемого ПК или сервера.

Вирусные мистификаторы (Hoaxes) — не являющиеся вредоносными почтовые сообщения, написанные в нейтральном тоне, где указывается, например, о якобы распространяющемся новом вирусе. Большинство вирусных мистификаций обладают одной или несколькими характеристиками:

1. Имя вируса, на которое ссылается автор сообщения, составляется не по правилам, используемым большинством антивирусных компаний.
2. Особо отмечается, что «вирус» пока не обнаруживается антивирусными программами. Пользователю предлагается найти некий файл и удалить его с диска.
3. В письме содержится призыв, в случае обнаружения указанного файла, сообщить об этом всем своим знакомым и все тем, чьи адреса есть в адресной книге пользователя.

Несмотря на всю безобидность подобного розыгрыша, вред его очевиден — массовая рассылка копий бесполезного сообщения загружает почтовый трафик и отнимает время пользователей.

«Горшочки с медом» (honey pots) — страницы-приманки, по описанию ресурса в поисковике и ключевым словам отвечающие требованиям поиска, на самом деле лишь завлекающие пользователя. Реально содержат на своих страницах всевозможные программы-эксплойты и различное нежелательное или вредоносное ПО.

Почтовые бомбы (Mail bombs) — один из простейших видов сетевых атак. Злоумышленником посылается на компьютер пользователя или почтовый сервер компании одно огромное сообщение или множество (десятки тысяч) мелких писем, что приводит к выводу системы из строя. В антивирусных продуктах Dr.Web для почтовых серверов предусмотрен специальный механизм защиты от таких атак.

Скамминг (Scamming) — от английского scamming, что означает «жульничество», вид интернет-мошенничества. Заключается в привлечении клиентов якобы брачными или другими агентствами (на самом деле скам-агентствами) с целью выуживания у них денег.

Ботнет (Botnet) — сеть зомбированных компьютеров, использующаяся для рассылки спама или сетевых атак, например, подбора паролей или DoS.

DNS poisoning — атака, базирующаяся на заражении кеша DNS-сервера жертвы ложной записью о соответствии DNS-имени хоста, которому жертва доверяет, и IP-адреса атакующего. Является подвидом спуфинга. Поражаться может как клиентский хост, так и хост сервера, что может привести к массовому перенаправлению пользователей на ложный адрес.

DoS-атаки (DoS-attacks) — или «отказ в обслуживании». Популярный у злоумышленников вид сетевых атак, граничащий с терроризмом, заключается в посылке огромного числа запросов с большого числа компьютеров на атакуемый сервер с целью выведения его из строя. При достижении определенного количества запросов (ограниченного аппаратными возможностями сервера) сервер перестает с ними справляться, что приводит к отказу в обслуживании. Как правило, такой атаке предшествует спуфинг. DoS-атаки стали широко используемым средством запугивания и шантажа конкурентов.

Сниффинг (Sniffing) — вид сетевой атаки, также именуемый «пассивное прослушивание сети». Несанкционированное сканирование сети и наблюдение за данными производятся при помощи специальной программы — пакетного сниффера, который осуществляет перехват всех сетевых пакетов домена, за которым идет наблюдение. Перехваченные таким снифферором данные могут быть использованы злоумышленниками для проникновения в сеть на правах фальшивого пользователя. Блокируется брандмауэром.

Спуфинг (Spoofing) — вид сетевой атаки, заключающейся в получении обманным путем доступа в сеть посредством имитации соединения. Используется для обхода систем управления доступом на основе IP-адресов, а также для набирающей сейчас обороты маскировки ложных сайтов под их легальных двойников или просто под законные бизнес-проекты. Блокируется брандмауэром.

Вишинг (Vishing) — технология интернет-мошенничества, разновидность фишинга, заключающаяся в использовании в злонамеренных целях war diallers (автодозвонщиков) и возможностей интернет-телефонии (VoIP) для кражи личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т. д. Потенциальные жертвы получают телефонные звонки якобы от имени легальных организаций, в которых их просят ввести с клавиатуры телефона, смарт-фона или КПК пароли, PIN-коды и другую личную информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы и в других преступлениях.

Атаки методом подбора пароля (Brute force attacks) — так называемые атаки методом «грубой силы». Как правило, пользователи применяют простейшие пароли, например "123", "admin" и т. д. Этим и пользуются компьютерные злоумышленники, которые при помощи специальных троянских программ вычисляют необходимый для проникновения в сеть пароль методом подбора — на основании заложенного в эту программу словаря паролей или генерируя случайные последовательности символов.

Фишинг (Phishing) — технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т. д. При помощи спамерских рассылок или почтовых червей потенциальным жертвам рассылаются подложные письма якобы от имени легальных организаций, в которых их просят зайти на подделанный преступниками сайт такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию, используемую в последствии злоумышленниками для кражи денег со счета жертвы. Разновидность социальной инженерии.

Фарминг — сравнительно новый вид интернет-мошенничества. Фарминг-технологии позволяют изменять DNS (Domain Name System) записи либо записи в файле HOSTS. При посещении пользователем легитимной, с его точки зрения, страницы, производится перенаправление на поддельную страницу, созданную для сбора конфиденциальной информации. Чаще всего таким способом подменяют страницы банков.

Технологии социальной инженерии — способы получения конфиденциальной информации у пользователей путем введения их в заблуждение. Очень часто это приводит к добровольной выдаче самими пользователями такой информации. Социальная инженерия не использует специальных компьютерных программ, мошенничество построено на тривиальном обмане, злоупотреблении доверчивостью и наивностью людей. Чаще всего рассылаются правдоподобно выглядящие письма от реально существующих кредитных организаций, в которых пользователя просят подтвердить пароль доступа к счету и PIN-код кредитной карточки.

Приложение 2. Полезные ссылки

Техническая поддержка Microsoft — *http://support.microsoft.com/search/default.aspx*
Рекомендации по безопасности от Mail.ru — *http://www.mail.ru/pages/help/183.html*
Обзор программ резервного копирования данных:

- *http://www.ixbt.com/soft/backup-part1.shtml*
- *http://www.ixbt.com/soft/backup-part2.shtml*
- *http://www.ixbt.com/soft/backup-part3.shtml*

Приложение 3. Как прислать вирус или сообщить о ложном срабатывании

Если вам в результате ручного поиска или посредством антивируса удалось обнаружить подозрительные или зараженные объекты, их непременно нужно отправлять в лабораторию «Доктор Веб». Сделать это можно несколькими способами:

- Зарегистрированные пользователи могут отправить вирус, обратившись в техническую поддержку. Для этого необходимо на начальной странице обращения (*https://support.drweb.com/support_wizard/?lng=ru*) выбрать пункт *Я являюсь зарегистрированным пользователем продуктов Dr.Web*, в появившихся полях указать ключевой файл (обычно: C:\Program Files\Drweb\drweb32.key) или серийный номер и нажать *Далее*. Затем выбрать пункт *Обнаружение или удаление вируса* и следовать указаниям мастера.
- Незарегистрированные пользователи могут воспользоваться ссылкой *Прислать вирус* на главной странице официального сайта антивируса (прямая ссылка: *https://vms.drweb.com/sendvirus/?lng=ru*), заполнив необходимые поля, прикрепив подозрительные файлы и нажав *Отправить*.

Если компонент SpIDer Gate пропустил вредоносную или запрещенную Родительским контролем ссылку, или ложно сработал на «чистом» сайте, информацию об этом также необходимо прислать в «Доктор Веб», воспользовавшись ссылкой *Сообщить о вредоносном сайте* на главной странице официального сайта антивируса (прямая ссылка: *https://support.drweb.com/new/urlfilter/?lng=ru*). Зарегистрированные пользователи могут сделать это, обратившись в службу технической поддержки, как это описано выше (выбрать пункт *Сообщить о ложном срабатывании Родительского контроля Dr.Web*).

Приложение 4. Глоссарий

ActiveX – технология связывания и встраивания объектов различных типов (например, вставка видеофайлов на веб-страницы).
Подробнее: *http://ru.wikipedia.org/wiki/Object_Linking_and_Embedding*.

Iframe – миниатюрный html-документ, который может отображаться в произвольном месте страницы (т. н. «плавающий фрейм»). Подробнее читайте на странице в разделе 5, на странице 23 и *http://ru.wikipedia.org/wiki/Iframe*.

IM-система – программа для мгновенного обмена сообщениями. Например: Skype, ICQ и т. д.

JavaScript – язык программирования, использующийся при написании клиентских (выполняемых на ПК пользователя, а не на сервере) скриптов.
Подробнее: *http://ru.wikipedia.org/wiki/JavaScript*.

MSconfig – системная утилита Windows, предназначенная для настройки параметров ОС. Подобнее о ней в разделе 5, на странице 26.

Netstat – программа, позволяющая через командную строку получить все сведения о текущих сетевых соединениях ПК. Отображается информация о том, какая программа использует какой порт, и каково его текущее состояние. Использование описано в разделе 5, на странице 23. Подробнее: *http://support.microsoft.com/kb/137984/ru*.

Process Explorer – менеджер процессов от компании Microsoft с широкими возможностями. Подробнее: *http://technet.microsoft.com/ru-ru/sysinternals/bb896653*.

Regedit – редактор реестра Windows. Для получения информации по программе нажмите *Пуск –> Выполнить –> regedit, OK*, и в открывшемся окне выберите *Справка –> Вызов справки*.

Shark режим – режим работы сканера Dr.Web, в результате которого пользователь получает отчет, который можно проанализировать. Применяется для поиска неизвестных вирусов. Подробнее читайте в разделе 9, на странице 33.

Trojan.Plastix fix – полное название утилиты для восстановления системы после разрушительных действий троянцев – plstfix.exe. Работа с ней описана в разделе 11, на странице 49.

UAC – средство контроля учетных записей пользователей. Подробнее: *http://ru.wikipedia.org/wiki/User_Account_Control*.

Автоматическое обновление Windows – системная функция Windows, позволяющая ей автоматически скачивать с сайта Microsoft и устанавливать обновления. Обновление устраняет выявленные ошибки в системе, повышая уровень надежности и безопасности работы.

Администратор (учетная запись) – главная учетная запись компьютера, имеющая максимально возможные права доступа. Установка некоторых программ и действий по настройке ПК требуется выполнять с этой учетной записи или другой, имеющей права администратора.

Аккаунт – то же, что и Учетная запись. Пара логин-пароль, присваиваемая пользователю какого либо интернет-ресурса или ПК и являющаяся его идентификатором, позволяющим совершать все действия непосредственно от своего имени. Подробнее: *http://ru.wikipedia.org/wiki/Аккаунт*.

Антивирусная программа (антивирус) – специальная программа, предназначенная для поиска и уничтожения вредоносных программ всех типов, а также для предотвращения их попадания на ПК, где эта программа установлена. Устанавливается как обычное приложение и постоянно активна во время работы компьютера.

Антивирусная утилита – отдельная утилита, не требующая установки и способная запускаться из любой папки компьютера. Выполняет те же базовые функции, что и антивирусная программа, но не осуществляет постоянной защиты.

Антифишинговый фильтр – функция, позволяющая программе (например, антивирусу или браузеру) блокировать заведомо ложные (фишинговые) ссылки.

Брандмауэр – то же, что Сетевой экран. Программа, осуществляющая контроль трафика, проходящего через ПК. Подробнее: *http://ru.wikipedia.org/wiki/Межсетевой_экран*.

Браузер – программа для просмотра веб-страниц. Подробнее: *http://ru.wikipedia.org/wiki/Браузер*.

Ветвь реестра – набор ключей реестра, относящихся к одному приложению или определенному набору свойств ОС (например, ветвь, отвечающая за параметры запуска программ). Название обусловлено древовидной структурой системного реестра Windows.

Вирус – вид вредоносного ПО, отличный от прочих тем, что способен самостоятельно размножаться, добавляя свои копии в файлы, тем самым инфицируя их и делая носителями вируса.

Вредоносное ПО – любое приложение (программа), которое может причинить вред компьютеру или его пользователю (кража данных, паролей, порча информации и т. д.).

Драйвер – служебная программа, необходимая для правильного функционирования какой-либо составляющей ПК. Например, драйвер видеокарты. Подробнее: *http://ru.wikipedia.org/wiki/Драйвер*.

Загрузочный сектор – начальная область диска, где хранится информация об алгоритме запуска компонентов ПК и ОС. Подробнее: *http://ru.wikipedia.org/wiki/Загрузочный_сектор*.

Зараженный ПК – компьютер, на котором имеется одна или несколько действующих вредоносных программ или вирусов.

Интернет-атака – действие, осуществляемое через сеть Интернет хакером с помощью различных уловок или специального ПО, направленное на кражу или повреждение данных. Целью интернет-атак может быть шпионаж, кража конфиденциальной информации или вандализм.

Карантин – папка, в которую антивирусная программа копирует пораженные и подозрительные файлы для дальнейшей отправки в антивирусную лабораторию. Файлы в этой папке, как правило, зашифрованы и лишены расширений, таким образом, находящиеся там вирусы опасности не представляют.

Киберпреступник – то же, что хакер. Преступник, деятельность которого направлена на повреждение или кражу электронных данных, таких как: электронные деньги, личные данные пользователей, конфиденциальная информация компаний.

Ключ реестра – запись в системном реестре Windows, имеющая название и содержание. Редактируя содержимое различных ключей реестра, можно управлять соответствующими им параметрами ОС или приложений.

Код разблокировки – код, который требуется ввести в отведенное поле для разблокировки ПК от вирусов семейства Trojan.Winlock. Подробнее в разделе 11, на странице 49.

Контрольная сумма – набор данных, однозначно соотнесенный с определенной версией файла. Контрольная сумма используется для проверки целостности файла и его подлинности. Подробнее: *http://ru.wikipedia.org/wiki/Контрольная_сумма*.

Папка Автозагрузка – системная папка Windows. Содержащиеся в ней программы или ярлыки загружаются в память ПК при входе пользователя в систему.

Перехват – технология, позволяющая сторонней программе вклиниваться в процесс выполнения другой программы, изменяя ее поведение. Подробнее: *http://ru.wikipedia.org/wiki/Перехват_(программирование)*.

Плагин – дополнение к какой-либо программе, расширяющее ее функционал. Например, плагин для Firefox, блокирующий рекламные блоки на сайтах. Подробнее: *http://ru.wikipedia.org/wiki/Плагин*.

Почтовый клиент – программа, позволяющая работать с электронной почтой. Подробнее: *http://ru.wikipedia.org/wiki/Почтовый_клиент*.

Реестр — главная база данных операционной системы Windows. В частности, позволяет вносить любые изменения в настройки системы и установленных приложений.
Подробнее: *http://ru.wikipedia.org/wiki/Реестр_Windows*.

Родительский контроль — функция, позволяющая ограничить доступ определенных пользователей к каким-либо папкам на локальном ПК или ресурсам сети Интернет. Например, с ее помощью можно заблокировать ребенку доступ на сайты, содержащие порнографию или насилие.

Руткит-технология — одна из технологий программной маскировки вредоносного действия вирусов. Подробнее читайте в разделе 5, на странице 24.

Сетевой порт — выделяемое программе виртуальное сетевое подключение. Технология сетевых портов позволяет нескольким программам одновременно использовать одно общее сетевое подключение. Подробнее: *http://ru.wikipedia.org/wiki/Порт_(TCP/IP)*.

Сеть — группа ПК, имеющих доступ к ресурсам друг друга посредством кабельного или беспроводного соединения. Локальные сети называются интрасетями, глобальная сеть — Интернет.

Скрипт — то же, что сценарий. Небольшая программа, написанная на скриптовом языке программирования. Скрипты могут функционировать только в соответствующих программных средах (как правило, в браузерах). Подробнее: *http://ru.wikipedia.org/wiki/Скрипт*.

Служба — сервисное приложение Windows, выполняющее определенные функции. Например, служба доступа к удаленному рабочему столу, и т. д.
Подробнее: *http://ru.wikipedia.org/wiki/Службы_Windows*.

Социальная инженерия — разновидность интернет-атаки, основанная больше на психологии, нежели на программных средствах взлома.
Подробнее: *http://ru.wikipedia.org/wiki/Социальная_инженерия_(безопасность)*.

Спам — нежелательная почта, зачастую рекламного характера. Также спам нередко содержит вирусы, вредоносные скрипты или ссылки на ресурсы с вредоносным ПО.
Подробнее: *http://ru.wikipedia.org/wiki/Спам*.

Съемный носитель — любой носитель информации, не имеющий постоянного жесткого соединения с ПК. К съемным носителям относятся USB-накопители, съемные жесткие диски, DVD-диски и т. д.

Троянец — разновидность вредоносного ПО. Подробнее в приложении 1, на странице 65.

Угроза — программа (см. Вредоносное ПО) или действие злоумышленника, направленное на причинение какого-либо вреда пользователю или его компьютеру. Это может быть мошенничество, кража данных, порча и уничтожение информации и т. д.

Уязвимость — ошибка в какой-либо программе, позволяющая ей или с ее помощью осуществлять доступ к функциям или компонентам ОС. Как правило, используется вредоносными программами или киберпреступниками.
Подробнее: *http://ru.wikipedia.org/wiki/Уязвимость_(компьютерная_безопасность)*.

Файл HOSTS — файл базы данных Windows, отвечающий за сопоставление IP-адресов доменным именам. Изменять его без необходимости не рекомендуется. Подробнее читайте в разделе 12, на странице 53.

Флешка — то же, что USB-накопитель. Переносное устройство для хранения данных.

Цифровая подпись — метод, позволяющий однозначно идентифицировать программу или документ как продукт определенного разработчика или автора. Используется для обеспечения безопасности, контроля целостности и борьбы с контрафактным ПО.
Подробнее: *http://ru.wikipedia.org/wiki/Цифровая_подпись*.