ГБПОУ ВО "Борисоглебский техникум промышленных
и информационных технологий"

Защита от вредоносного программного обеспечения

Материалы по дисциплине «Техническое обслуживание СВТ»
Специальность «Компьютерные системы и комплексы»
Автор: Торгашин Р.Г

2017

Оглавление

Вредоносные программы 3
Определение 3
Для чего люди пишут вредоносное ПО? 3
Каким бывает вредоносное ПО? 5
Популярные методы внедрения вредоносных программ 10
Эксплуатация методов социальной инженерии 11
Эксплуатация уязвимостей 13
Эксплуатация ошибок администрирования 14
Использование джойнера. 18
Использование символов юникода 19
Профилактика 20
Своевременная установка обновлений безопасности для программ и операционной системы 20
Использование и настройка встроенных средств безопасности 22
Распределение и контроль прав пользователей 24
Установка и настройка антивирусного ПО 24
Регламентирование работы пользователя 26
Выбор антивирусного программного обеспечения 28
Симптомы заражения 40
Заболел - лечись! 42
Список источников 46

Вредоносные программы

Определение

В статье 273 Уголовного кодекса Российской Федерации сказано «Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.» То есть под вредоносными понимаются все программы предназначенные уничтожения, блокирования, модификации и копирования информации и нейтрализации средств защиты – если эти действия выполняются без ведома пользователя. В дальнейшем будем считать вирус частным случаем вредоносной программы.

Формально, вирусы – самовоспроизводящийся программный код, который может самостоятельно размножаться заражая другие системы. Но сейчас на бытовом уровне принято называть вирусами все вредоносные программы.

Для чего люди пишут вредоносное ПО?

От пользователей часто можно услышать вопрос - Зачем люди пишут компьютерные вирусы? В чем "профит"? Ответ на это вопрос интересен не только с "философской" точки зрения но и с точки зрения практики, так как от цели написания вредоносного ПО может зависеть его поведение в системе, симптомы заражения и т.п.

Как показывает практика цель написания вирусов:

Самореклама - чтобы, заразив максимально большое число систем продемонстрировать свои навыки потенциальным заказчикам. Такие вирусы стараются вести себя "тихо" до определенного момента, чтобы заразить как можно больше систем до обнаружения.

Часто они не повреждают данные и не доставляют каких-либо серьезных проблем ине связаны с требованием денег. К этой категории можно отнести программы шутники (joker), вред от которых заключается в периодическом выводе на экран сообщений, открытии лотка оптического привода и т.п.

Вандализм - как и в первом случае, цель автора не в получении денег. Но эти вирусы ориентированы на повреждение данных и оборудования. К этой категории можно отнести вирусы стирающие или перезаписывающие неадекватными данными файлы

(например троян Penetrator). "Скрытый" период таких вирусов недолог и их активизация част сопровождается выводом сообщений.

Кража данных - одна из самый, пожалуй, распространенных целей. Такое программное обеспечение максимально маскируется в системе и старается ничем себя не проявить. Ведь от того, насколько долго вирус не будет замечен зависит объем украденных данных. Может быть опознано косвенно - по паразитному сетевому трафику и компрометации данных. Украденные данные могут потом использоваться автором вируса, могут быть проданы третьим лицам или за их удаления у хозяина потребуют денег. Данные могут быть любыми: логины и пароли, данные кредитных карт, личные фото и видео файлы, коммерческие секреты.

Вымогательство денег (ransomware) - еще одна все более популярная цель. Такие вирусы воруют данные или каким-либо образом блокируют к ним доступ и вымогают у хозяина деньги за удаление украденных копий или возращение доступа. Сейчас наиболее популярен с шифрованием данных. Атакам подвергаются не только частные лица или коммерческие учреждения но и медицинские центры.

Так например по время эпидемии WannaCry атака коснулась медицинских учреждений в Лондоне, а также английских городах Блэкберн, Ноттингем и графствах Камбрия и Хартфордшир. Из-за атаки некоторые медучреждения предупредили, что будут принимать только экстренных пациентов.

Важно понимать, что выплаты авторам таких вирусов бессмысленны. Во-первых потому, что нет гарантии их "честности". Они могут не вернуть доступ даже получив деньги. Более того, новые поколения таких вирусов шифруют данные уникальным вновь сгенерированным ключом, и потом удаляют его, так что даже автор вируса не может расшифровать.

Целевая атака - в целом целевая атака может иметь черты любой другой. Чаще всего это кража данных или атака на работоспособность серверов. Отличительной чертой является то, что атаке подвергается только одна цель - фирма или другая организация за нападение на которую заплатили.

Организация ботнета - сама по себе такая атака не влияет на работу системы. Цель ее в том, чтобы установить программное обеспечение которое позволит атаковать другие компьютеры/серверы по команде хозяина ботнета. Такое ПО старается не проявлять себя и обычно не вредит данным или работе системы. Однако использование зараженной системы опасно для сети и других компьютеров, поэтому провайдер может применить санкции вплоть до отключения!

Каким бывает вредоносное ПО?

Файловые вирусы - вирус, который может *самостоятельно* внедрятся в другие файлы. При этом во время запуска программы (или загрузке офисного документа для редактирования) вирус получает управление. Получив управление вирус записывает свой код внутрь выполняемого файла и изменяет его таким образом, чтобы после запуска файла управление получил код вируса. Файловый вирус может записать свое тело во все другие файлы, хранящиеся на диске компьютера.

От таких вирусов частично помогает выполнение нехитрого правила: не запускать исполняемые файлы и не открывать документы полученные из ненадежного источника.

Для внедрения могут использоваться различные технологии[1].

Метод добавления новой секции

Это самый распространённый метод заражения файлов, не утрачивающий своей популярности вопреки его успешному обнаружению всеми антивирусами. Суть данного метода заключается в добавлении секции в конец исполняемого файла. Далее, вирус пересчитывает размер образа всего файла, выставляет на секцию нужные флаги, включая флаг исполнения (0x20000000), и меняет точку входа на начало новой секции.

При запуске заражённого файла сначала выполнится код из вирусной секции, а затем произойдет переход на оригинальную точку входа.

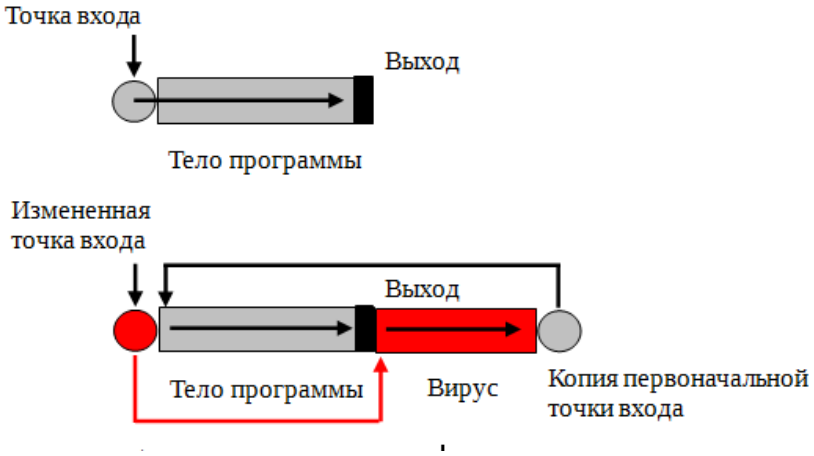

Рисунок 1 Метод добавления новой секции

[1] http://www.nobunkum.ru/ru/file-infectors

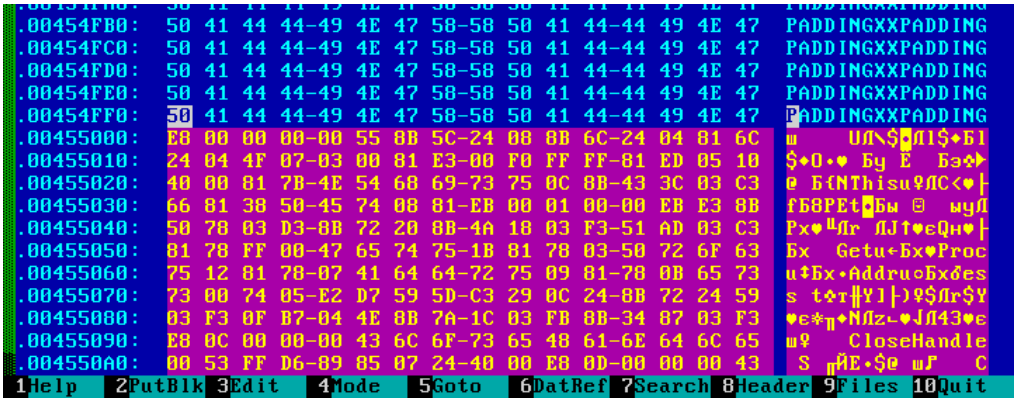

Рисунок 2 Фрагмент кода зараженного файла

На рисунке видно, что после кода для выравнивания, оставленного компилятором в конце файла идет осмысленный код, содержащий точку входа. Это является очевидным признаком заражения.

Для лечения файлов, заражённых описанным методом, достаточно удалить последнюю секцию и восстановить оригинальную точку входа

Расширение последней секции

Это также один из наиболее популярных методов заражения исполняемых файлов. Вирус получает указатель на последнюю секцию исполняемого файла и увеличивает её атрибуты физического размера и виртуального размера, тем самым расширяя секцию. Затем вирус пересчитывает размер образа и выставляет на последнюю секцию нужные флаги, включая флаг исполнения (0x20000000), вычисляет новую точку входа и заменяет оригинальную.

Заражение методом EPO (Entry Point Obscuring)

Для осуществления заражения вирус ищет в секции, из которой начинается выполнение программы, опкод инструкции типа call (E8) или jmp (E9), после чего подставляет в эту инструкцию адрес перехода на вирусный код. Последний при этом может храниться в произвольном участке файла: в расширенной последней секции, в добавленной секции, в конце последней секции и т.п.

Модификация секций

Манипулирование секциями исполняемого файла является более искусным методом заражения. Могут использоваться две разновидности данного метода.

В первом случае вирус внедряет свой код вместо секции с таблицей переадресаций и перенаправляет на него точку входа. После того, как внедренный код отработал, вирус восстанавливает в памяти оригинальную секцию переадресаций, а затем передает управление на OEP.

Метод со сдвигом секции ресурсов применим только к файлам, в которых эта секция является последней. В таком случае вирус заражает своим кодом предпоследнюю секцию в файле, предварительно сдвинув секцию ресурсов.

Заражение динамической библиотекой

Суть данной техники заключается в том, что код вируса располагается в отдельной динамической библиотеке, а переход на него из зараженного файла происходит путем вызова функции, экспортируемой из этой библиотеки.

Метод «украденных байт»

Метод «украденных байт» — техника передачи управления вирусному коду, как и в случае с методом EPO.

В большинстве случаев вирусы изменяют оригинальную точку входа. Вместо этого можно «украсть» несколько байт оригинального кода программы, вставив вместо них инструкцию перехода на вредоносный код. Обычно подменяются байты в начале программы.

Загрузочные вирусы - вирусы, который записывает свой код в главную загрузочную запись Master Boot Record диска или загрузочную запись Boot Record диска и дискет.

Загрузочный вирус активизируется после загрузки компьютера. Он получает управление до программы загрузки ОС, в результате чего процедура загрузки выполняется под контролем вируса.

При заражении загрузочный вирус заменяет загрузочную запись или главную загрузочную запись. Настоящая загрузочная запись или главная загрузочная при этом запись обычно не пропадает (хотя так бывает не всегда). Вирус копирует их в один из свободных секторов.

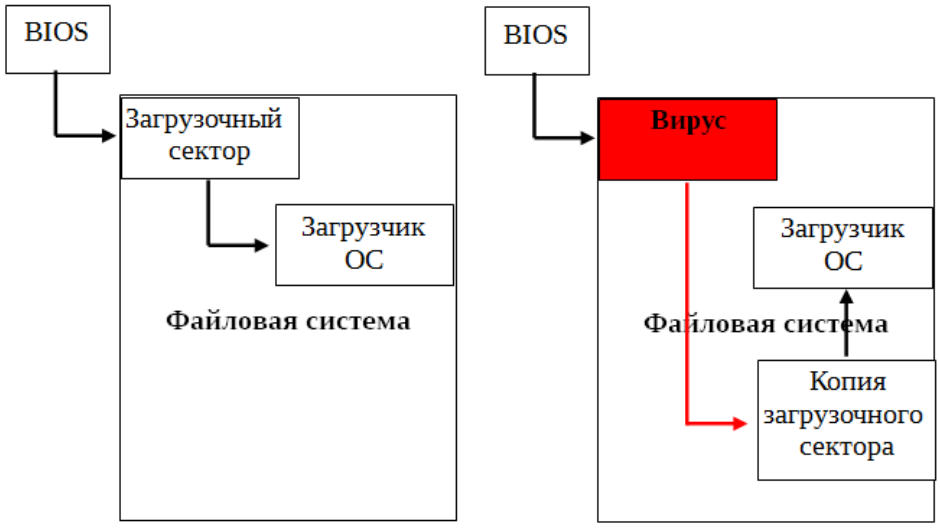

Рисунок 3 Принцип работы загрузочного вируса

Макрокомандные вирусы (макровирусы) (Macroviruses) - вирусы, заражающие файлы документов, обрабатываемых приложениями Microsoft Office и другими программами, допускающие 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 так называемый общий шаблон NORMAL.DOT и макросы, помещенные в общий шаблон автоматически запускаются при открытии любого документа. Учитывая то, что копирование макросов из документа в документ (в частности в общий шаблон) выполняется всего одной командой, среда Microsoft Word идеальна для существования макрокомандных вирусов.

Чтобы защититься от таких вирусов не нужно открывать документы полученные из ненадежного источника и отключить в настройка офисных программ атоматический запуск макросов.

Вирусы-черви - компьютерная программа, способная копировать себя с одной машины на другие. Компьютерные черви могут использовать ошибки конфигурации сети (например, чтобы скопировать себя на полностью доступный диск) или бреши в защите операционной системы и приложений. Многие черви распространяют свои копии через сеть несколькими способами.

Защитой от таких вирусов является использование сетевых экранов (firewall)

"Троянские кони", «Трояны» - это программа, наносящая какие-либо разрушительные действия, т. е. в зависимости от определенных условий или при каждом запуске уничтожающая информацию на дисках, "приводящая" систему (к зависанию) и т. п. Большинство известных "троянских коней" подделываются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. В последние годы популярной стала подделка плагинов для веб-браузеров, например flash-player’a, java script и т.п.

Трояны не самовоспроизводятся и не распространяются сами по себе. Однако с увеличением объема информации и файлов в Интернете трояном стало довольно легко заразится.

Рисунок 4 Часть дампа памяти Backdoor.Win32.Bredolab

Специфическим видом троянских программ являются ***НОАХ программы***. Идея Ноах-программ — обман пользователя, чаще всего с целью получения прибыли или похищения конфиденциальной информации. В последнее время наблюдается тенденция криминализации этой отрасли: если еще год назад большинство Ноах-программ производили сравнительно безобидные действия, имитируя заражение компьютера вирусами или SpyWare-кодом, то современные все чаще нацелены на похищение паролей или конфиденциальной информации. Пример такой программы показан на рисунке

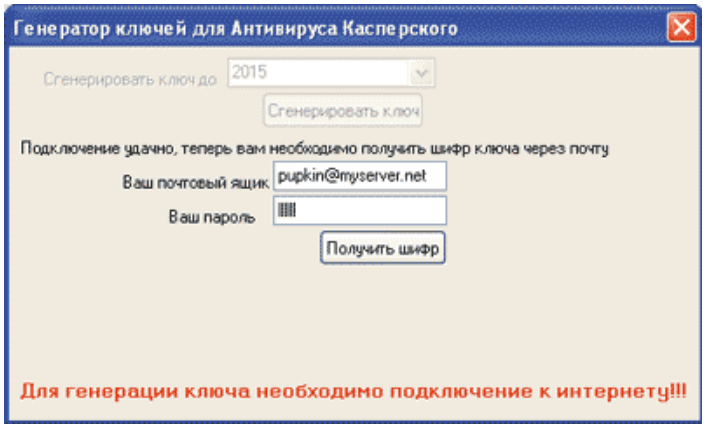

Рисунок 5 Окно программы Hoax.Win32.Delf

Как следует из окна программы и ее описания, это генератор лицензий для «Антивируса Касперского». Программа предлагает для получения сгенерированной лицензии ввести адрес своей электронной почты и пароль на доступ к почтовому ящику. Если доверчивый пользователь сделает это и нажмет кнопку «Получить шифр», то введенные им данные будут переданы злоумышленнику по электронной почте.

Очевидно, что защита от таких вирусов - не скачивать и не запускать ПО в происхождении которого не уверен.

Руткиты (rootkit) - программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

В системах Windows под rootkit принято подразумевать программу, которая внедряется в систему и перехватывает системные функции (Windows API). Перехват и модификация низкоуровневых API-функций, в первую очередь, позволяет такой программе достаточно качественно маскировать свое присутствие в системе. Кроме того, как правило, rootkit может маскировать присутствие в системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие rootkit устанавливают в систему свои драйверы и службы (они также являются "невидимыми").

В системах на базе Linux и прочих *nix ядер руткиты являются одной из основных угроз. Заражение классическими вирусами в этих системах затруднено из-за специфической архитектуры. В то же время такие системы более критичны к квалификации администратора. Поэтому появляется определенный простор для целенаправленного внедрения руткита за счет использования ошибок администрирования.

Вирусы - компаньоны - данный вирус создает для файла пользователя файл-двойник, при этом код файла-жертвы не изменяется. Обычно вирус изменяет расширение файла (например, с .exe на .com) и назначает ему атрибуты скрытый и системный, потом создает свою копию с именем, идентичным имени файла-жертвы, и дает ему расширение, тоже идентичное. Ничего не подозревающий пользователь запускает любимую программу и не подозревает, что это вирус. Вирус, в свою очередь, заражает еще несколько файлов и запускает программу, затребованную пользователем.

Могут быть подменены не только программы но и документы. Если в ОС отключено отображение расширений, то файл с именем **важныйдокумент.docx.exe** будет выглядеть как вполне легальный **важныйдокумент.docx.** Особенно если вирус позаботился заменить и пиктограмму.

Эпидемия вирусов такого типа заражающих флэш накопители была недавно - так называемые autorun вирусы скрывали папки и файлы, а свои копии выдавали за них. После лечения такого накопителя создается впечатление что данные утрачены. Но по объему занятого места видно что это не так.

Чтобы защититься от такого заражения можно включить отображение расширений файла и скрытых и системных файлов.

Популярные методы внедрения вредоносных программ

Для организации эффективного противодействия внедрению вредоносных программ важно понимать механизм такого внедрения.

На стадии заражения вредоносная программа должна выполнить следующие задачи:

- запуститься в атакуемой системе;
- повысить свой права до максимально возможных. В идеальном случае – получить права суперпользователя/администратора или получить статус модуля ядра системы. Какие методы могут использоваться для решения этих задач?

Эксплуатация методов социальной инженерии

Методы социальной инженерии тем или иным способом заставляют пользователя скачать и/или запустить заражённый файл, открыть ссылку на заражённый веб-сайт . Эти методы применяются почтовыми червями и другими видами вредоносного программного обеспечения.

Задача хакеров и вирусописателей — привлечь внимание пользователя к заражённому файлу (или HTTP-ссылке на заражённый файл), заинтересовать пользователя, заставить его кликнуть по файлу (или по ссылке на файл).

«Классикой жанра» является нашумевший в мае 2000 года почтовый червь ILOVEYOU, известный также как LoveLetter, В общей сложности, вирус поразил более 3 миллионов компьютеров по всему миру. Предполагаемый ущерб, который червь нанёс мировой экономике, оценивается в размере 10-15 миллиардов долларов, за что вошёл в Книгу рекордов Гиннесса, как самый разрушительный компьютерный вирус в мире.. Сообщение, которое червь выводил на экран, выглядело следующим образом:

Рисунок 6 Почтовый клиент с письмом отправленным вирусом ILOVEYOU

Для защиты от такого заражения пользователю достаточно не открывать файлы прикрепленные к электронным сообщениям и не переходить по ссылкам в том числе в соц.сетях, если он не уверены на 100% в происхождении этих файлов и ссылок.

Несмотря на это такой способ внедрения вредоносных программ все еще эффективен. Например его использует как основной путь распространения троянская

программа CryptoLocker. Она внедряется в поддельные письма в виде исполняемого файла замаскированного под документ в формате PDF, DOCX или т.п. Часто письма отправляются от имени известных служб, например FedEx and UPS tracking notifications[2].

Популярным в последнее время стало предложение пользователю скачать некоторое программное обеспечение необходимое для просмотра видео, защиты от вирусов и т.п. В этом случае пользователю предлагается ссылка для скачивания, переход по которой приводит к скачиванию зараженного файла или трояна. Часто для маскировки используются названия реально существующих и известных программ и модулей. В этом случае поддельная ссылка может вести на фишинговый сайт имитирующий сайт производителя ПО.

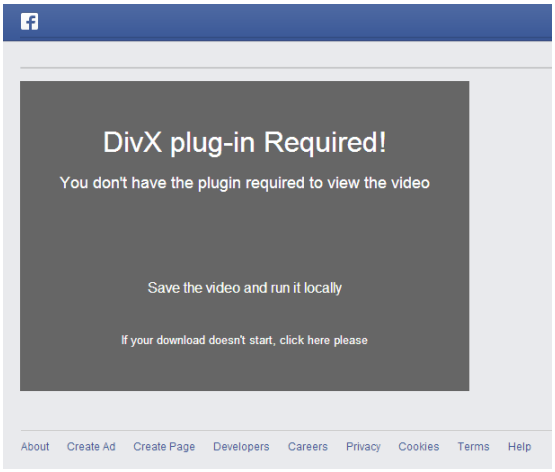

Рисунок 7 Сообщение о необходимости загрузить плагин DivX со ссылкой на файл зараженный Trojan.Tofsee

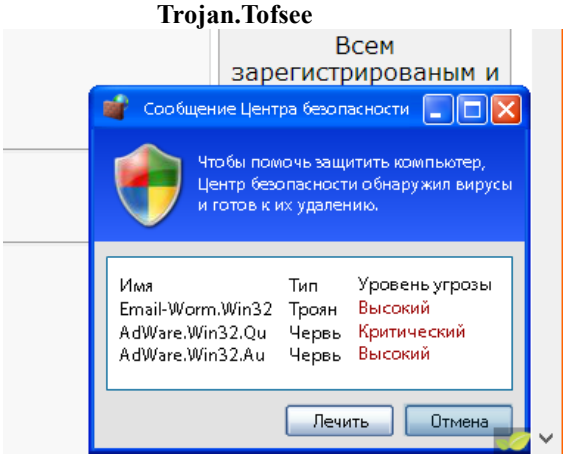

Рисунок 8 Всплывающее окно в браузере имитирующее сообщение центра безопасности WndowsXP

Само построение фишинговых сайтов, то есть внешне не отличимых от настоящих применяется в различных видах интернет – мошенничества. Но это выходит за рамки нашего исследования.

[2] CryptoLocker Virus: New Malware Holds Computers For Ransom, Demands $300 Within 100 Hours And Threatens To Encrypt Hard Drive [Электронный ресурс]. - Режим доступа: http://www.ibtimes.com/cryptolocker-virus-new-malware-holds-computers-ransom-demands-300-within-100-hours-threatens-encrypt

Чтобы избежать заражения по такой схеме пользователь не должен скачивать программы, утилиты и плагины с сторонних сайтов. Нужно скачивать их с сайта производителя.

Эксплуатация уязвимостей

Эти технологии используются злоумышленниками для внедрения в систему вредоносного кода скрытно, не привлекая внимания владельца компьютера. Осуществляется это через уязвимости в системе безопасности операционных систем и в программном обеспечении. Наличие уязвимостей позволяет изготовленному злоумышленником сетевому червю или троянской программе проникнуть в компьютер-жертву и самостоятельно запустить себя на исполнение.

Уязвимости являются, по сути, ошибками в коде или в логике работы различных программ. Современные операционные системы и приложения имеют сложную структуру и обширный функционал, и избежать ошибок при их проектировании и разработке просто невозможно. Этим и пользуются вирусописатели и компьютерные злоумышленники.

Уязвимостями в почтовых клиентах Outlook пользовались почтовые черви Nimda и Aliz. Для того чтобы запустить файл червя, достаточно было открыть заражённое письмо или просто навести на него курсор в окне предварительного просмотра.

Также вредоносные программы активно использовали уязвимости в сетевых компонентах операционных систем. Для своего распространения такими уязвимостями пользовались черви CodeRed, Sasser, Slammer, Lovesan (Blaster) и многие другие черви, работающие под ОС Windows. Под удар попали и Linux-системы — черви Ramen и Slapper проникали на компьютеры через уязвимости в этой операционной среде и приложениях для неё.

В последние годы одним из наиболее популярных способов заражения стало внедрение вредоносного кода через веб-страницы. При этом часто используются уязвимости в интернет-браузерах. На веб-страницу помещается заражённый файл и скрипт-программа, которая использует уязвимость в браузере. При заходе пользователя на заражённую страницу срабатывает скрипт-программа, которая через уязвимость закачивает заражённый файл на компьютер и запускает его там на выполнение.

Уязвимости, о которых становятся известно, достаточно оперативно исправляются компаниями-разработчиками, однако постоянно появляется информация о новых уязвимостях, которые тут же начинают использоваться многочисленными хакерами и вирусописателями.

Многие троянские «боты» используют новые уязвимости для увеличения своей численности, а новые ошибки в Microsoft Office тут же начинают применяться для внедрения в компьютеры очередных троянских программ. При этом, к сожалению, имеет место тенденция сокращения временного промежутка между появлением информации об очередной уязвимости и началом её использования червями и троянцами. В результате компании-производители уязвимого программного обеспечения и разработчики антивирусных программ оказываются в ситуации цейтнота. Первым необходимо максимально быстро исправить ошибку, протестировать результат (обычно называемый «заплаткой», «патчем») и разослать его пользователям, а вторым — немедленно выпустить средство детектирования и блокирования объектов (файлов, сетевых пакетов), использующих уязвимость.

Уменьшить вероятность заражения в этом случае можно оперативно устанавливая обновления операционной системы и программного обеспечения.

К сожалению, на 100% обезопасить себя от такого пути заражения невозможно.

Эксплуатация ошибок администрирования

Часто причиной заражения систему вредоносным кодом становятся не ошибки архитектуры или программной реализации (кода) а ***неверные настройки или несвоевременное выполнение профилактических операций.*** То - есть ошибки администрирования.

Следует сразу отметить тот факт, что наибольшую известность получили случаи эксплуатации ошибок администрирования OS Windows. Это связано с тем, что Windows имеет более низкий порог вхождения и активно используется на компьютерах конечных пользователей. Поэтому она часто администрируется низкоквалифицированным персоналом.

В то же время Linux-based системы в большей степени используются на серверах, рабочих станциях, производственном оборудовании и имеют более высокий порог вхождения. Поэтому такие системы чаще администрируются специалистами высоко квалификации. Однако то, что для качественного администрирования таких систем требуется более глубокое знание архитектуры – приводит к специфическим ошибкам администрирования. Что касается операционных систем фирмы Apple то они более защищены благодаря использованию закрытой архитектуры.

Таким образом большая часть примеров которые мы будем приводить – относится именно к этой операционной системе. ***Но это не значит, что Linux – based системы и MacOS на 100% защищены от таких атак.***

Косвенно об этом говорит ситуация с смартфонами на базе ОС Android. Эта система построена на базе Linux. Но как только доля устройств с этой ОС стала достаточно большой и через них стало возможно снимать деньги с банковских счетов - появились методы взлома и заражения. Этому способствуют пользователи, которые снимают защиту "рутованием" устройств. Отсюда видно, что если заражать систему выгодно и она обслуживается низкоквалифицированным персоналом - заражением вполне возможно.

К ошибкам администрирования можно отнести.

Использование «слабых» паролей (weak password) пользователей и/или использование политик администрирования позволяющих задавать такие пароли.

Различные антивирусные лаборатории и специалисты по компьютерной безопасности регулярно публикуют списки наиболее часто используемых паролей[3]. Примечательно, что состав этих списков мало изменяется. Вредоносные программы, при попытке получения прав доступа к системе, могут проверять такие пароли. Например так работает вирус Worm:Win32/Morto.A[4].

Кроме того, слабые, короткие пароли, даже сохраненные в виде хэшей, могут быть подобраны с помощью простого перебора (brute force) или радужных таблиц (rainbow table). Понятно, что использование «пустых» паролей или «семейного» входа в систему тем более недопустимо.

Несовременная установка обновлений операционной системы и программ.

Как уже говорилось выше – любое программное обеспечение содержит уязвимости. Чтобы лишить вирусописателей возможности их использовать регулярно выпускаются обновления. Если администратор системы отключил автоматическую установку обновлений и не медлит с ручной установкой – это повышает риск заражения. Например известный вирус Net-Worm.Win32.Kido для заражения компьютера использует уязвимости в службе сервера и протоколе SMB ОС Windows 2000-Windows7. Эти уязвимости закрываются патчами описанными в бюллетенях MS08-067, MS08-068, MS09-001[5]. Если данные патчи не установлены система может быть заражена данным вирусом, причем многие антивирусные программы не детектируют заражение.

---

[3] Top 25 most commonly used and worst passwords of 2013 [Электронный ресурс]. - Режим доступа: http://www.networkworld.com/article/2226175/microsoft-subnet/top-25-most-commonly-used-and-worst-passwords-of-2013.html

[4] Microsoft Malware Protection Center Worm:Win32/Morto.A [Электронный ресурс]. - Режим доступа: http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Morto.A

[5] Как бороться с сетевым червем Net-Worm.Win32.Kido [Электронный ресурс]. - Режим доступа: http://support.kaspersky.ru/viruses/disinfection/1956#block0

Прогремевший в 2017 году вирус Wanacry использовал дыру в протоколе SMB. И чтобы спастись от него нужно было установить патч.

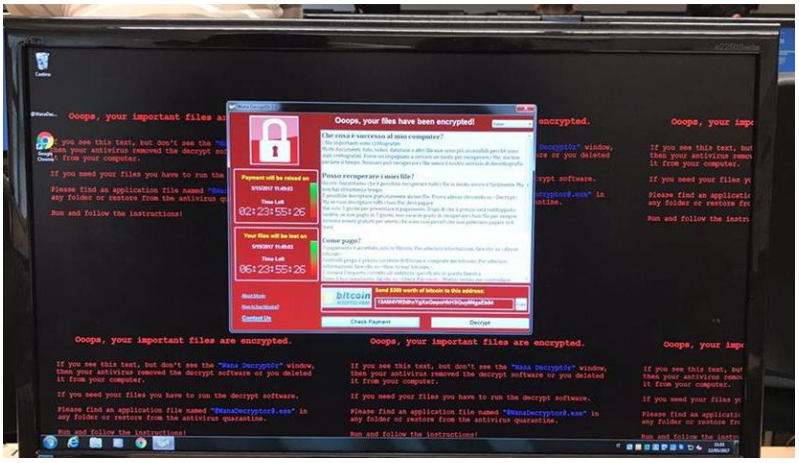

Рисунок 9 Экран компьютера зараженного Wanacry

Несвоевременная установка обновлений может быть причиной заражения не только Windows так и других ОС. Например Heartbleed – ошибка переполнения буфера в OpenSSL позволяющая прочитать память клиента или сервера в том числе закрытый ключ сервера. Этой ошибка подвержены многие дистрибутивы RedHat, Debian, SUSE и т.д. если не установлен патч CVE-2014-0160.

Неверное распределение прав между пользователями.

Обычно причиной заражения становится выделение излишне разрешающих прав. Сюда же можно отнести использование пользователем входа в систему обладающего расширенными правами (администратор) без веской причины. В большинстве операционных систем если процесс запускается пользователем или другим процессом – он получает права и окружение запустившего. Например, если пользователь запускает браузер или торрент-клиент, скачивает с их помощью файл и открывает его через интерфейс браузера (торрент-клиента), то запущенный для этого процесс получает права пользователя. Таки образом, если пользователь обладал правами администратора, скачанный файл будет выполнен с правами администратора. Если этот файл заражен, вредоносная программа сразу получает полные права на доступ к системе. Если же пользователь имел ограниченные права – вредоносная программа должна попытаться получить их каким-либо способом.

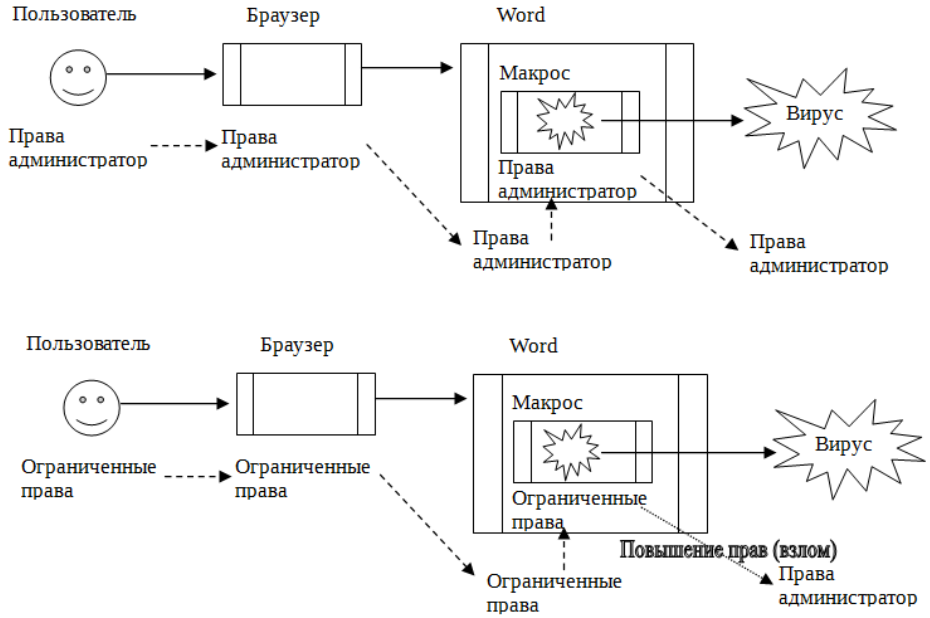

Рисунок 10 Получение макросом прав администратора через их наследование от пользователя

Низкоквалифицированные пользователи работают с правами администратора постоянно. Они считают что это облегчает использование компьютера. По опыту работы хочется заметить, что за 5 лет действительно оправданное использование мною прав администратора составило в среднем 1-2 раза в месяц. Из этих случаев в примерно 80% случаев достаточно оказалось запустить программу от имени администратора.

Неверное конфигурирование или отказ от использования механизмов защиты, встроенных в операционную систему и программное обеспечение.

Существует возможность блокировать запуск неизвестных программ, так называемые «белые» и «черные» списки программ. В Windows Vista появился User Account Control - этот компонент запрашивает подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера а механизм «черных» и «белых» списков улучшен и включен в состав «родительского контроля». Очевидно, что если в системе разрешен запуск только определенного списка приложений – вероятность запуска вредоносной программы и дальнейшего заражения – резко снижается.

Часто администраторы операционных систем идут на поводу у пользователей и отключают встроенные механизмы защиты, так как те «мешают». В то же время опыт эксплуатации UAC и белых списков говорит о том, что рядовой пользователь на полностью настроенном компьютере сталкивается с ними не чаще нескольких раз в месяц.

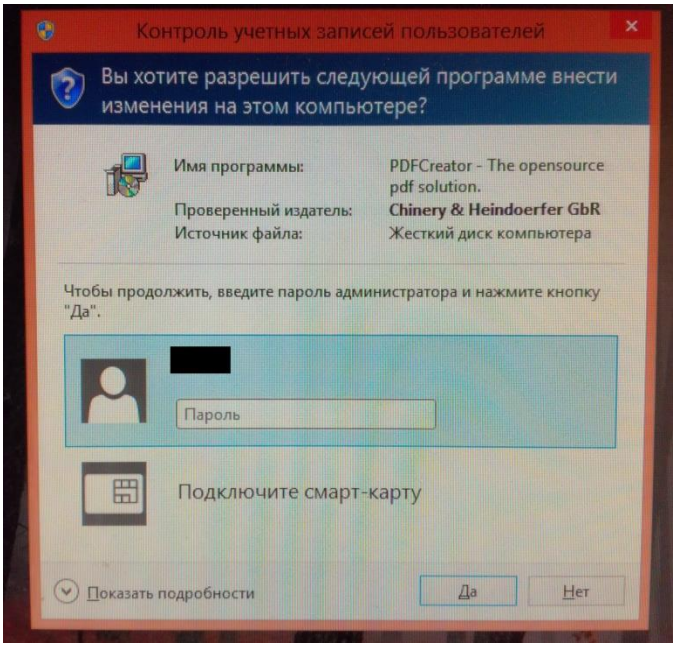

Рисунок 11 Окно UAC

Многие вредоносные программы не ограничиваются одним методом внедрения, а используют их комбинации. Тем не менее, с точки зрения защиты это не имеет большого значения, так как грамотно построенная система противодействия вторжению должна противостоять всем методам. В этом случае вредоносная программа не сможет проникнуть в систему даже если будет использовать все известные методики вторжения.

Использование джойнера[6].

Джойнер (joiner) — программа, которая позволяет “склеивать” вредоносную программу с любым файлом в конечный формат “.exe”. Таким образом, взяв, к примеру, дистрибутив программы 2ГИС, становится возможным связать его с вирусом и отправить как обычный инсталлятор обычному пользователю.

Самым простым джойнером является любой архиватор (например, WinRAR). Архиваторы имеют функцию создания самораспаковывающихся архивов SFX, у которых на выходе расширение “.exe”. Таким образом, в архив добавляются два исполняемых файла и запаковываются. Далее, остаётся методом простого обмана заставить пользователя компьютера открыть данный архив и с этого момента процесс не обратим.

К слову, антивирусы никак не реагируют на данный метод склейки файлов, так как он считается легальным. SFX-архивы используются в повсеместном использовании, хоть и не так часто, как это было задумано. Разработчики антивирусов не берут во внимание тот факт, что данным способом также пользуются в корыстных целях.

---

[6] Рудниченко А. К., Шаханова М. В. Актуальные способы внедрения компьютерных вирусов в информационные системы // Молодой ученый. — 2016. — №11. — С. 221-223.

Использование профессионального джойнера никак нельзя отследить на готовом файле с расширением “.exe”. В таком случае лучше обезопасить себя, скачивая необходимые программы с официальных сайтов разработчиков. Что касается джойнера SFX-архивом, то его можно отследить, попробовав открыть готовый файл архивом. Если открывается архив без каких-либо ошибок, значит подозрения оправдываются.

Использование символов юникода[7].

Юникод — один из стандартов кодирования символов. Позволяет представить знаки почти всех письменных языков. Операционная система Windows поддерживает символы юникода в названиях файлов. А так как, Windows является самой распространённой системой на ПК, то значит и злоумышленник имеет некоторое преимущество перед жертвой.

Юникод в название файла добавить очень просто, достаточно вызвать контекстное меню и выбрать нужный символ как на рисунке. В нашем случае, это код RLO (Начать отмену справа налево).

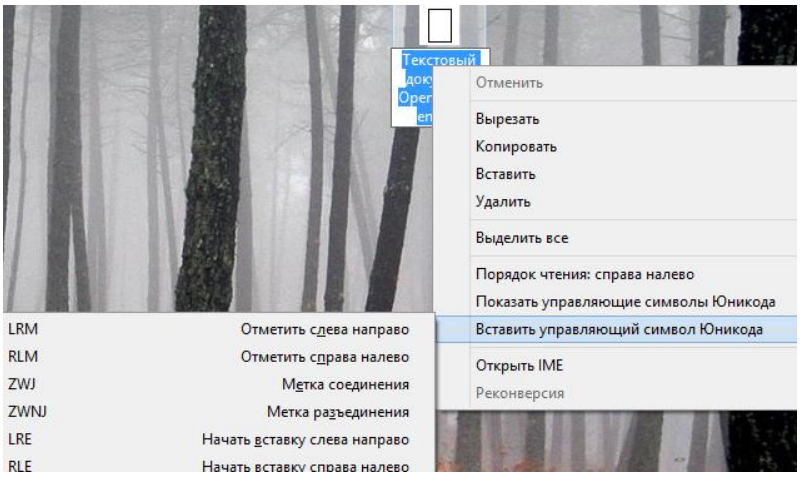

Рисунок 12 Демонстрация вставки символа юникода RLO

Суть данного кода — зеркалирование символов после вставленного кода. Например, файл имеет название “TESTgpj.exe”, вставив RLO после “TEST”, то получим: “TESTexe.jpg”. Смысл перестановки расширений файлов в том, что обычный пользователь в первую очередь посмотрит на расширение файла, чтобы не заразить свой компьютер. Жертва, руководствуясь своими базовыми знаниями, поймёт, что это изображение (формат “.jpg”) и отбросит всякие подозрения.

[7] Рудниченко А. К., Шаханова М. В. Актуальные способы внедрения компьютерных вирусов в информационные системы // Молодой ученый. — 2016. — №11. — С. 221-223.

Антивирусные программы также бессильны в данном случае, так как просто-напросто не проверяют названия файлов на символы юникода в нём. Данная функция в операционной системе Windows является стандартной.

В случае юникода в имени файла проверить подлинное расширение можно через меню “Свойства”. Графа “Тип файла”. Если там написано “Приложение (.exe)”, то стоит задуматься.

Профилактика

Как и в случаях с заболеваниями биологических объектов, заражение вредоносным ПО проще предупредить, чем бороться с ним. Утраченные уникальные данные восстановить будет невозможно.

Поэтому важно выполнять комплекс профилактических мер. В приведенном ниже списке все пункты обязательны. Не выполнение какого-либо из них может свести к 0 остальные усилия.

Комплекс мер

- Своевременная установка обновлений безопасности для программ и операционной системы;
- Использование и настройка встроенных средств безопасности;
- Распределение и контроль прав пользователей;
- Установка и настройка антивирусного ПО;
- Регламентирование работы пользователя.

Что нужно сделать для выполнения каждого пункта?

Своевременная установка обновлений безопасности для программ и операционной системы

Наиболее эффективной является политика, при которой критические обновления и обновления системы безопасности ставятся автоматически.

Единственной допустимой причиной переключения обновлений в режим «проверка в ручную» может быть частое использований компьютера в условиях. когда получение обновлений затруднено. Например, если отсутствует стабильное подключение к информационным сетям или для подключения используется тариф с высокой ценой за скачанный объем информации. В таких случаях администратор должен обеспечить регулярную доставку обновлений иными способами.

В Windows обновление компонентов системы и обновление программного обеспечения разделено. Для обновления системы используется утилита Microsoft Windows Update а для обновления программного обеспечения – утилиты в составе самих программ. Поэтому администратор должен настроить периодичность обновлений для каждой программы и для операционной системы.

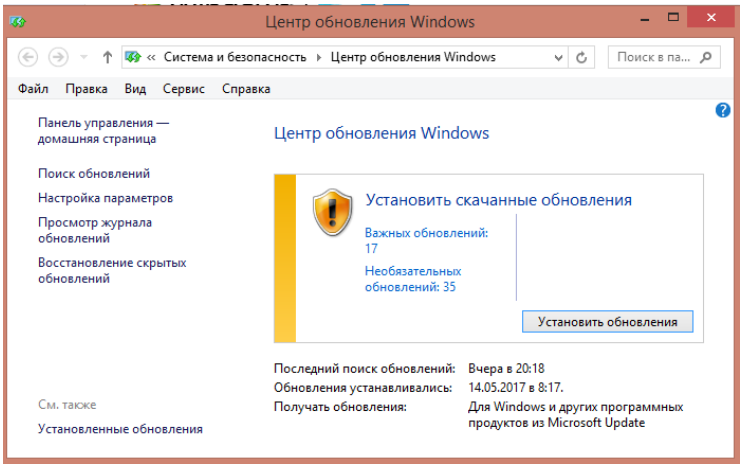

Рисунок 13 Окно Microsoft Windows Update

Чтобы запустить интерфейс Microsoft Windows Update нужно перейти в

Панель управления\Система и безопасность\Центр обновления Windows

или набрать команду

control /name Microsoft.WindowsUpdate

Важно помнить, что Microsoft Windows Update по умолчанию работает от имени пользователя SYSTEM и обладает правами администратора системы, кроме того он не блокируется UAC. Поэтому установка обновлений Windows может происходить незаметно для пользователя. Единственное, что должен предусмотреть администратор – некоторым обновлениям нужна перезагрузка системы. Если такая перезагрузка может привести к потере данных пользователя – следует переключить ее в «ручной» режим.

Настройка автоматического обновления стороннего программно обеспечения может быть сопряжена с трудностями. Подавляющее большинство программ для установки своих обновлений требуют прав администратора и блокируются системой UAC. Примером такой программы является утилита обновления Java. Более того, в случае с Java Updater, даже разрешение через UAC не позволяет корректно обновить ПО если у пользователя нет прав администратора.

Для программ, которые не могут проверять обновления - администратор должен обеспечить проверку и установку обновлений вручную.

В Linux – based дистрибутивах использующих менеджеры пакетов, таких как Debian, Ubuntu, RedHat, Suse, Fedora – обновления всех компонентов системы и программного обеспечения выполняется менеджером пакетов. Это обеспечивает больший уровень автоматизации. Администратор системы настраивает регулярный запуск менеджера пакетов на проверку и установку обновлений.

Например для Debian-based дистрибутивов можно воспользоваться утилитой cron-apt. Менеджер автоматически проверяет репозитории и устанавливает обновления, попутно проверяя контрольные суммы и подписи этих программ.

Или вручную настроить запуск по cron команд

apt-get update

apt-get upgrade

apt-get dist-upgrade

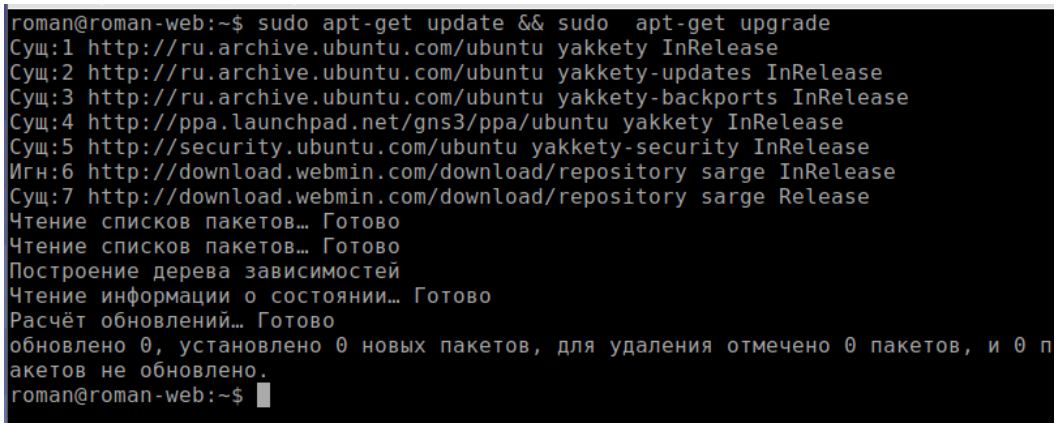

Рисунок 14 Ubuntu - Установка обновлений вручную

Периодичность проверки обновлений устанавливается исходя из условий эксплуатации и задач системы. Рекомендуется проверка обновлений системы раз в день и установка обновлений по мере появления.

Использование и настройка встроенных средств безопасности

Встроенные в систему средства безопасности настраиваются администратором. Возможность настройки и отключения таких систем обычными операторами является серьезным нарушением.

Для защиты от вредоносных программ администратор должен настроить следующие средства.

Политики паролей. Нужно указать максимальный срок после которого пользователь должен будет сменить пароль. Указать сколько паролей подряд не могут

повторятся. Эти параметры определяются исходя из задач пользователя. Указать минимальную длину паролей, в настоящее время считается что длинна должна быть по крайней мере 6 символов. Включить требования сложности для паролей.

Политики входа в систему. Указать сколько раз пользователь может ввести неверный пароль. Включить требование нажатия Ctrl+Alt+Del. Запретить вход без пароля.

Встроенный брандмауэр/файрволл. Наиболее безопасной является конфигурация которая запрещает все соединения кроме явно разрешенных администратором. В этом случае разрешают соединения для программ использование которых необходимо для решения задач пользователя. Обычно это браузер, утилита автоматического обновления. Кроме того разрешают использование некоторых портов, необходимых для работы программ и служб. В последнем случае следует убедится, что с разрешаемым портом уже связан доверенный процесс. Иначе вредоносная программа может назначить себе разрешенный порт.

Многие сетевые экраны могут работать в режиме «обучения» когда при установлении незарегистрированного соединения пользователю предлагается выбрать действие: запретить, разрешить однократно, создать правило. Администратору следует по возможности отключать режим обучения, если только он не уверен в достаточной квалификации оператора.

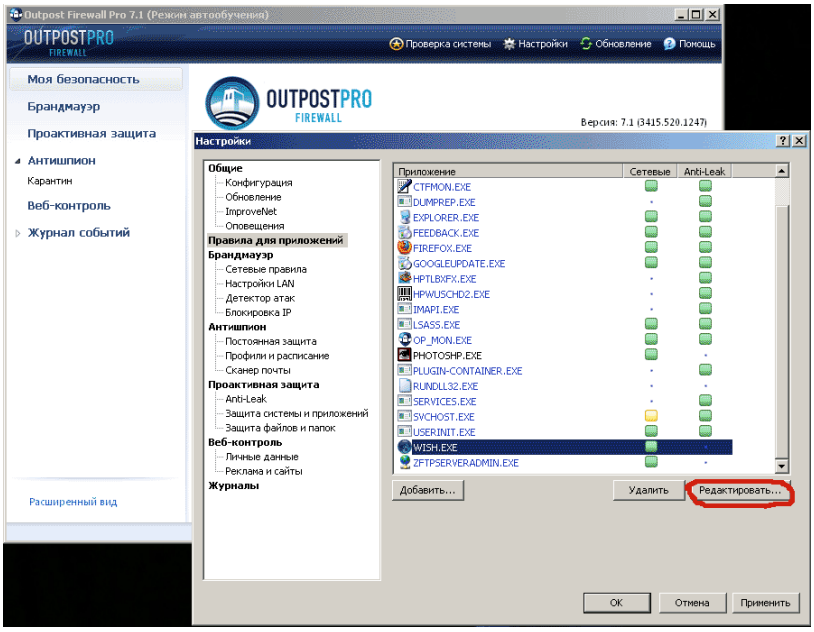

Рисунок 15 Окно настроек программы Outpost

«Белые» и «черные» списки. Под «черными» списками обычно понимают список программ и процессов запуск которых система блокирует. Такие списки мало эффективны в защите от вредоносных программ, так как вызывает сомнение возможность составить список всех подобных программ и зараженных ими исполняемых файлов.

Использование «белых» списков напротив, весьма эффективно. При настройке такого списка система разрешает запуск только тех программ и процессов имена которых явно указаны. Сравнительно не трудно составить список программ, которые необходимы для решения задач пользователя и работы системы.

Контроль подписей файлов. В целях защиты от подмены передаваемого файла и его заражения в процессе передачи могут использоваться подписи файлов различными сертификатами безопасности. В операционные системы Windows и Linux-based включены утилиты обеспечивающий контроль таких сертификатов для драйверов и исполняемых файлов.

Распределение и контроль прав пользователей

Выполнение этого условия позволяет обезопасить систему в случае нарушения пользователем регламента работы. Кроме того в случае проникновения в систему вредоносной программы через сессию пользователя имеющего ограниченные права, программа должна повысить свои права, иначе она не сможет эффективно работать. Администратор системы должен распределить права доступа и настроить политики безопасности исходя из следующих соображений:

- уровень прав пользователя должен соответствовать его задачам и квалификации. Ни один пользователь не должен иметь прав больше, чем ему необходимо для выполнения его задач.
- использовать аккаунты с повышенными права и аккаунты администраторов можно только тогда, когда этого нельзя избежать. Постоянная работа с правами администратора недопустима.
- все пользователи для входа должны использовать устойчивые пароли. Возможность входа в систему без пароля должна быть исключена.

Установка и настройка антивирусного ПО

Крайне необходимо использовать антивирусное ПО если система работает под управлением ОС Windows. Это связано с тем что подавляющее число вредоносного ПО написано для это операционной системы.

Теоретически, квалифицированный пользователь может, настроив все механизмы безопасности вплоть дл белых списков и пристально следя за каждым своим действием, не использовать антивирус. Но это ведет в неоправданным затратам времени и сил. Кроме того

"ассортимент" вирусов так велик, что запомнить все их характерные черты не реально. А рекомендовать отказ от антивируса неквалифицированным пользователям - -бессмысленно.

В то же время нужно понимать, что это не панацея. И без соблюдения остальных правил антивирус окажется неэффективным.

Подробнее о антивирусах и их выборе речь пойдет ниже.

Настройки антивирусных программ могут отличаться по названию и по составу. Но определенные базовые настройки совпадают по смыслу. **На какие же настройки нужно обратить внимание?**

Расписание автоматической проверки

Автоматическая проверка является важным элементом защиты системы. Различают:

быструю проверку - проверяются только критически важные области, такие как оперативная память, загрузочная область и т.п

полную проверку - проверяются все носители и области.

выборочную проверку - проверка областей по выбору пользователя.

Важно настроить расписание проверок. Ясно, что быстрая проверка должна выполнятся чаще полной. Насколько часто проводить проверку зависит от конкретных условий. При определении расписания важно помнить, что любая проверка сильно нагружает ресурсы системы. Поэтому разумно проводить ее в период, когда техника простаивает.

Например можно настроить быструю проверку ежедневно с 12.00 - обеденный перерыв. А полную - на вечер пятницы, после окончания рабочего дня. В последнем случае удобно настроить так, чтобы компьютер автоматически выключался после завершения проверки.

Расписание обновления баз и программы

Чем чаще обновляются базы, тем быстрее антивирус получит сигнатуры новых вирусов и сможет защитить от них компьютер. Поэтому самым разумным является настройка **ежедневной** установки обновлений и проверки обновлений программ.

Единственной причиной более редкого обновления может быть отсутствие стабильного Интернет канала.

В сложных случаях многие **программы позволяют устанавливать ранее скаченые обновления "вручную"**.

Настройки мониторинга

Мониторинг должен быть включен постоянно!

Если для каких-то программ известно, что они вызывают ложное срабатывание антивируса - их можно исключить из проверки и мониторинга. Для этого в антивирусе есть специальный интерфейс. Предварительно нужно убедиться в том, что срабатывание действительно ложное.

Некоторые антивирусы позволяют настроить максимальную нагрузку на процессор, которую будет создавать средство мониторинга. Это может происходить непосредственно или за счет указания максимального объема проверяемого файла. Такая настройка позволяет использовать антивирус на маломощных компьютерах.

Важно помнить, что если в системе установлены несколько антивирусов - мониторинг должен быть включен только у одного.

Настройки файрволла/брандмауэра

В состав большинства антивирусов входит файрволл. Нужно помнить, что он может повлиять на работоспособность программ. Особенно если они используют сетевые соединения. Чтобы проверить так ли это нужо на время отключить файрволл. Если проблема с программой исчезнет - включить ее в список исключении файрволла.

Регламентирование работы пользователя

Это пункт подразумевает формулирование определенных правил работы с системой и следование этим правилам. Основной задачей регламентирования является противодействие использованию методов социальной инженерии и распространенбию троянских программ. Рассмотрим какие правила должны соблюдаться оператором для профилактики заражения системы.

Во первых ни один файл, который может быть заражен не должен редактироваться, копироваться, или другим способом обрабатываться в системе без предварительной проверки. Проверка может осуществляться антивирусными программами. Если для незараженного файла известна контрольная сумма или он подписан сертификатом безопасности это тоже можно использовать для проверки. **К потенциально опасным файлам относятся**:

- **исполняемые файлы** – в Windows это файлы с расширениями имен .com и .exe (.COM • .EXE (MZ / NE / LE / LX / PE / W3)), а также файлы, загружаемые при выполнении других программ, как то- файлы динамических библиотек, ресурсы, оверлейные файлы. То есть файлы с расширениями .com, .exe, .dll, .drv, .scr, .ovl. В Linux исполняемые файлы являются текстовыми с меткой исполняемых. Фактически исполняемым для данного пользователя считается любой файл у которого в правах

доступа стоит «x». Кроме того опасность могут представлять файлы скриптов исполняемых программами интерпретаторами. Это файлы для flash – .swf; JavaScript - .js; Java – jar.

- **файлы документов, содержащие программы на макроязыке** – документы в форматах Microsoft Office - .doc, .docx, .xls, .xlsx; форматах LibreOffice/OpenOffice - .odt, .ods. Долгое время безопасным считался формат rtf. Однако, как было установлено[8], существует возможность записать в документ ссылку на удаленный web сайт, содержащий шаблон, зараженный макро-вирусом. При чтении RTF-файла MS Word автоматически и без каких-либо предупреждений загрузит этот шаблон и незаметно запустит вирус.
- **графические файлы** – подлинные файлы графически форматов являются сравнительно безопасными. Хотя случаи встраивания вирусов в JPG файлы были зафиксированы,. это является экзотикой. Гораздо чаще под видом графического файла маскируется исполняемый с расширением jpg или bmp. Например filename.jpg.exe. Современные файловые менеджеры по умолчанию не отображают расширения файла и пользователь видит filename.jpg.
- **«подозрительные» файлы**. В связи с тем, что существуют способы «маскирования» исполняемых файлов под видом файлов безобидных форматов, следует считать подозрительными файлы:
  - объем которых сильно отличается от среднего для файлов подобного формата;
  - файлы, пиктограмма которых не соответствует формату;
  - файлы. полученные из ненадежного источника.

Из сказанного можно сделать вывод, что условно-безопасными на данный момент остался только формат TXT, Все остальные файлы должны проверятся перед использованием.

Во вторых, электронные письма, полученные из неизвестного или ненадежного источника и содержащие вложения не открывать. Если такое письмо все же надо открыть его следует предварительно проверить. Если письмо пришло из известного источника но без предварительной договоренности и содержит вложения – следует связать с источником и уточнить факт отправки такого письма.

В третьих, не следует посещать веб сайты с сомнительным контентом: «пиратские», содержащие информацию по взлому программ, порнографического характера и т.п.

[8]Обманчивая безопасность RTF-файлов [Электронный ресурс]. - Режим доступа: http://www.kaspersky.ru/about/news/virus/2001/Obmanchivaya_bezopasnost_RTF-failov

В четвертых, если какая-то программа или веб сайт предлагают установить модуль/плеер или любую другую программу следует отказаться от такой установки. Если этот модуль действительно необходим, следует скачать его с сайта производителя.

В пятых если квалификации оператора достаточно для разбора url адреса – следует обращать внимание на адреса сайтов чтобы избежать использования фишинговых страниц. Если при переходе на страницу «внутри» сайта сменился домен – такая страница является подозрительной.

Также нужно обращать внимание если браузер выдает сообщение о некорректном SSL сертификате. В этом случае нужно убедится, что домен предоставивший сертификат заслуживает доверия. Если квалификации пользователя недостаточно для такого анализа следует обратится к администратору или сотруднику службы безопасности.

Рисунок 16 Сообщение Chrome о предоставлении сервером ненадежного сертификата

В шестых – следует обращать внимание на возникновение симптомов заражения системы

Выбор антивирусного программного обеспечения

Выбор антивирусной программы, как и любой другой коммерческий вопрос, является «холиварной» темой. Споры по поводу того какая программа лучше не утихают давно и утихать не собираются. Во многом это связано с деятельностью маркетинговых отделов фирм-производителей антивирусов. С другой стороны, часто отмечается низкая квалификация спорящих.

Споры о выборе антивируса доходят до заявлений о том, что вирусы написаны самими компаниями производителями антивирусного ПО. Подобные «теории заговора» не стоили бы упоминания, если бы им не верило большое число неспециалистов. Тем, кто склоняется к такому же мнению предлагаю подумать над следующим:

Появление первых вирусов произошло не позднее 1980 года. Значит в 2017 году этой теме уже около 40 лет! К слову, большинство фирм, выпускающих антивирусное ПО,

существуют гораздо меньшее время. Например, антивирус DrWeb создан в 1992 году а компания в 2003[9]. А Лаборатория Касперского существует того меньше - с 2007 года[10].

Ну допустим, что до этого времени вирусы выпускали другие компании (может быть Symantec? Как раз основана в 1982).

Главный вопрос – как за сорок лет факт выпуска вирусов производителями антивирусного ПО ни разу не был подтвержден? Это прибыльный бизнес. И если бы конкуренты или независимые эксперты узнали о таком факте и могли предъявить доказательства – это было бы обнародовано*! Но таких случаев не было*.

Существует мнение, что можно использовать компьютер без антивирусного ПО и не заразить его. В некоторых случаях это верно.

Например, в 2017 году сравнительно безопасно использовать Linux-base операционные системы. Это связано с несколько более «продвинутой» системой безопасности и тем, что пока Linux используется на небольшом числе систем – написание вируса под него нерентабельно.

Также, можно обезопасить систему если:

выполнять все перечисленные выше рекомендации – устанавливать обновления, разграничить права доступа и так вплоть до настройки белых списков,

быть достаточно квалифицированным, чтобы определить потенциальную угрозу.

Но, во-первых, далеко не каждый пользователь обладает достаточной квалификацией. Во-вторых, работать в таких условиях – значит тратить довольно много сил и времен на анализ происходящего.

Кроме того, человек не может утверждать, что его система не заражена, так как многие вирусы никак не проявляются, а анализировать все файлы системы пользователь не в состоянии. ***Такой компьютер становится угрозой для сети и других компьютеров***.

Понятно, что заражение возможно и при наличии антивирусного ПО. Но вероятность его – меньше.

Поэтому отказ от использования антивируса в Windows – удел немногих энтузиастов.

Структура антивирусного программного обеспечения.

Антивирусное программное обеспечение обычно состоит из следующих компонентов:

[9] https://company.drweb.ru/?lng=ru
[10] https://www.kaspersky.ru/about

Монитор - служба постоянно находящаяся в памяти системы и непрерывно контролирующая ее работу. Эта служба проверяет изменяющиеся файлы, отслеживает обращения к системным библиотекам и т.п. Для экономии ресурсов системы проверка проводится в "облегченном" варианте.

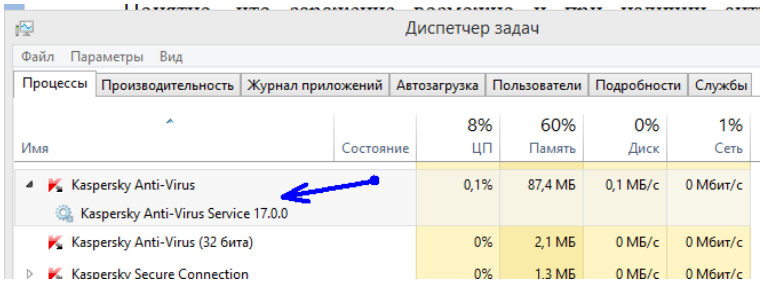

Рисунок 17 Служба мониторинга Kaspersky Anti-Virus

Антивирусный сканер - программа проверяющая файлы и критические области в памяти системы "по требованию". Такая проверка проводится по расписанию или запросу пользователя. Она выполняется в "полном" режиме. Следует заметить, что и монитор и сканер используют одно программное ядро и одни и те же базы сигнатур.

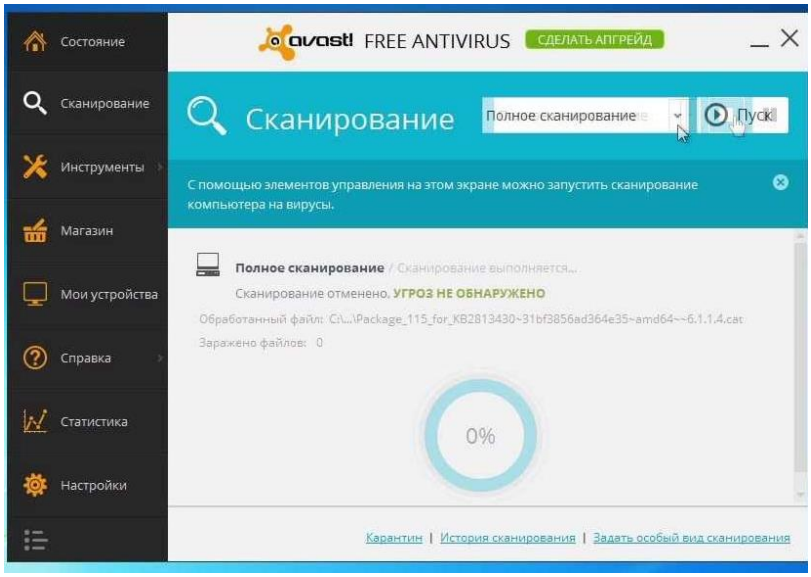

Рисунок 18 Сканирование антивирусом Avast

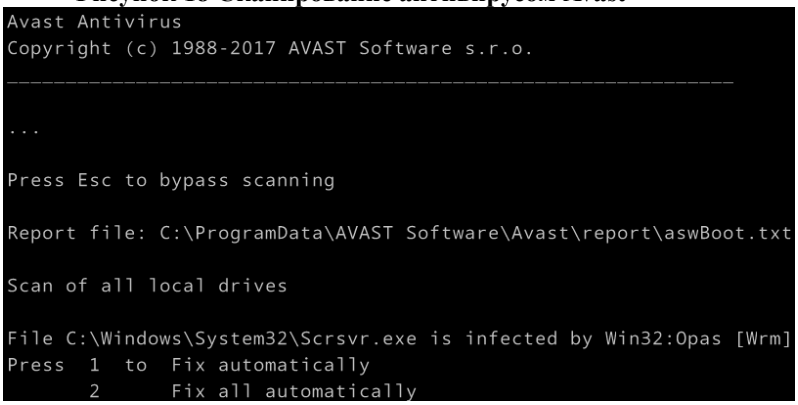

Рисунок 19 Сканирование антивирусом Avast при старте системы

В последнее время есть тенденция выносить проверку подозрительных файлов (или всех файлов) в облако. В этом случае антивирус отправляет файлы для проверки на сервер компании. Там они проверяются и сервер возвращает свое заключение. Такой подход снижает нагрузку на систему пользователя и обеспечивает компанию информацией о новых вирусах и вирусных эпидемиях. Однако такой антивирус хорошо работает если у пользователя хороший канал в Интернет и сервера компании не перегружены.

Интерфейс пользователя - утилита позволяющая пользователя управлять настройками антивируса.

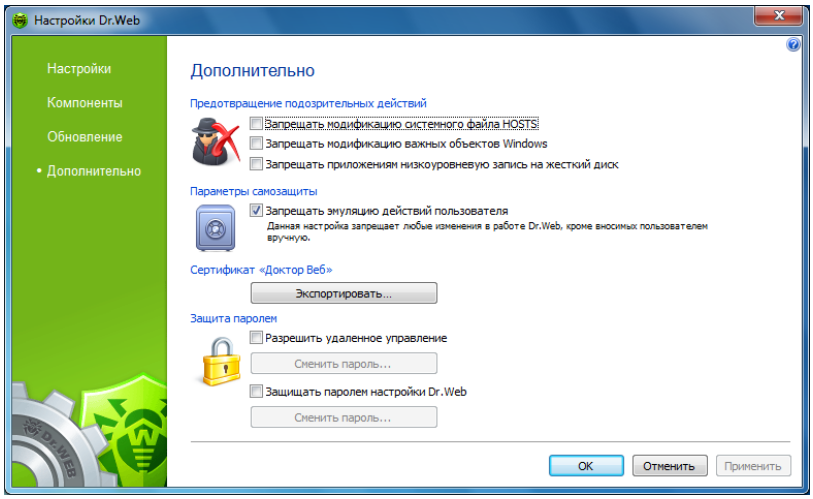

Рисунок 20 Интерфейс настроек DrWeb

Утилита обновления - утилита отвечающая за обновление антивирусных баз и программы.

Дополнительно в состав антивирусного программного пакета может входить: файрволл и другие функции.

Файрволл (межсетевой экран) - программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами[11].

Файрволлы входящие в состав антивирусных программ имеют ограниченный функционал и их назанчение - фильтрация трафика между ПК клиента и сетью. Они блокируют сетевые вызовы от процессов, которые пользователь или авторы антивируса не одобрили явно. Это защищает данные от кражи. И блокируют вызовы извне, вплоть до ICMP пакетов. Что обеспечивает защиту от внедрения червей и т.п.

[11] https://ru.wikipedia.org/wiki/Межсетевой_экран

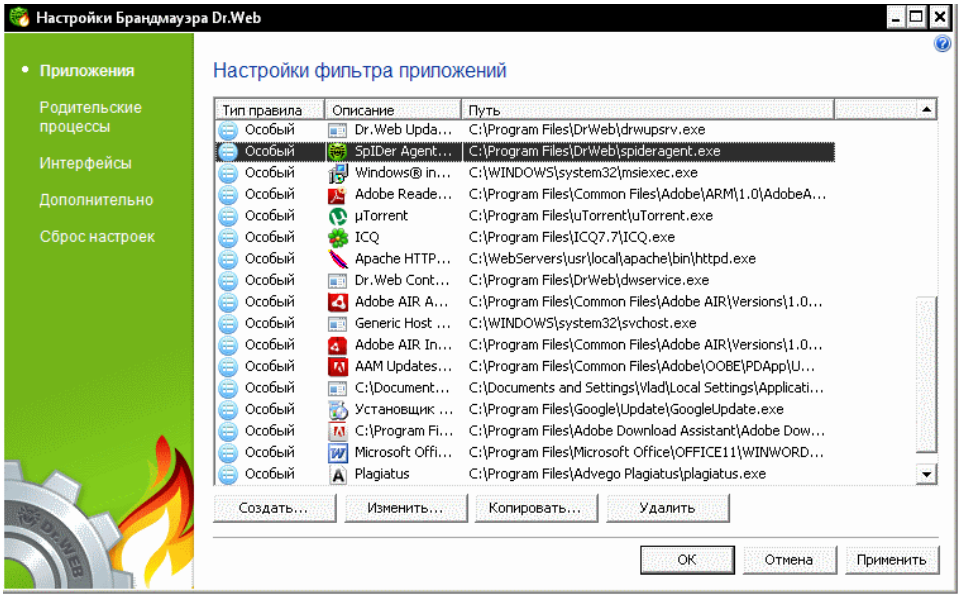

Рисунок 21 Настройки брандмауэра DrWeb

Здесь не будет рекомендовано конкретное антивирусное ПО. Оно должно выбираться исходя из конкретных условий эксплуатации системы.

Но ***рассмотрим параметры, по которым нужно выбирать антивирус***.

1. Качество детектирования вирусов по известным сигнатурам.

Обнаружение, основанное на сигнатурах — метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в словаре[12].

Для достижения достаточно продолжительного успеха при использовании этого метода необходимо периодически пополнять словарь известных вирусов новыми определениями – обновлять антивирусные базы.

Хотя антивирусные программы, созданные на основе поиска соответствия определению вируса в словаре, при обычных обстоятельствах могут достаточно эффективно препятствовать вспышкам заражения компьютеров, авторы вирусов стараются держаться на полшага впереди таких программ-антивирусов, создавая «олигоморфические», «полиморфические» и самые новые «метаморфические» вирусы, в которых некоторые части участки кода перезаписываются, модифицируются, шифруются или искажаются так, чтобы невозможно было обнаружить совпадение с определением в словаре вирусов.

[12] https://ru.wikipedia.org/wiki/Обнаружение,_основанное_на_сигнатурах

На практике, все более-менее известные антивирусы одинаково хорошо определяют вирусы сигнатуры, которых есть в ИХ базах. По крайней мере это относится к первым 10-20 программам в рейтингах.

Более важным в работе по известным сигнатурам является следующий параметр

2. Скорость внесения сигнатур вирусов в базы и полнота баз

Очевидно, что ***от того, сигнатуры скольких вирусов есть в базах и насколько быстро сигнатуры новых вирусов появляются в базе экземпляра антивирусной программы зависит надежность защиты.***

Традиционно для обновления баз скачиваются файлы с описаниями с сервера авторов антивируса. Расписание скачивания пользователь может настроить сам. В этом случае рекомендуется указать периодичность скачивания около раза в день.

Но даже если пользователь укажет периодичность обновления – раз в час все будет упираться в то, как быстро информация о новых угрозах окажется на сервере.

Разработка сигнатур — ручной процесс, тяжело поддающийся автоматизации.

Сигнатуры антивирусов создаются в результате кропотливого анализа нескольких копий файла, принадлежащего одному вирусу. Сигнатура должна содержать только уникальные строки из этого файла, настолько характерные, чтобы гарантировать минимальную возможность ложного срабатывания — главный приоритет любой антивирусной компании.

В этой ситуации часто выигрывают крупные компании предлагающие платные решения. Это связано с тем, что у них есть возможность оплатить работу большего коллектива квалифицированных специалистов.

3. Качество детектирования вирусов на основании эвристического анализа

Эвристический анализ (эвристическое сканирование) — это совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ, но в то же время этот же термин обозначает один из конкретных способов[13].

Практически все современные антивирусные средства применяют технологию эвристического анализа программного кода. Эвристический анализ нередко используется совместно с сигнатурным сканированием для поиска сложных шифрующихся и полиморфных вирусов. Методика эвристического анализа позволяет обнаруживать ранее

[13] https://ru.wikipedia.org/wiki/Эвристическое_сканирование

неизвестные инфекции, однако, лечение в таких случаях практически всегда оказывается невозможным. В таком случае, как правило, требуется дополнительное обновление антивирусных баз для получения последних сигнатур и алгоритмов лечения, которые, возможно, содержат информацию о ранее неизвестном вирусе. В противном случае, файл передается для исследования антивирусным аналитикам или авторам антивирусных программ, а в сканируемой системе удаляется или помещается в карантин.

От того, насколько хорошо работают используемые антивирусом эвристические алгоритмы зависит многое. Слишком «простые» алгоритмы могут быть обмануты. Слишком «подозрительный» алгоритм даст большое число ложных срабатываний. Поэтому подробность реализации эвристики является важным ноу-хау производителей.

В настоящее время качество реализации эвристики – одна из основных отличительных характеристик.

Уровень нагрузки на ресурсы системы

То, насколько много ресурсов требуется для работы антивирусной программы – важный фактор определяющий возможность ее использования.

Конечно, с точки зрения пользователя, чем меньше нагрузка, тем лучше. Однако нужно понимать, что антивирус должен проверять все файлы, которые копируются, изменяются или перемещаются между уровнями памяти системы. Он должен следить за тем, какие программы обращаются к системным вызовам, перехватывают прерывания и т.п. Понятно, что ***работа антивируса всегда требует ресурсов системы***.

Нет прямой зависимости между нагрузкой на ресурс и качеством работы, так как многое зависит от качества кода антивируса. Но нужно понимать, что ***антивирус, который «совсем» не потребляет ресурсы – не работает.***

Важно разделять уровень нагрузки при постоянном мониторинге и уровень нагрузки при полной проверке системы. Полная проверка проводится редко, ее можно запланировать на свободное время и с высокой нагрузкой можно смирится.

В целом, администратор должен решить какой баланс между надежностью и нагрузкой на ресурс подходит в конкретном случае.

Но он должен понимать, что если работа антивирусного монитора почти полностью блокирует выполнение задач пользователя -то зачем нужен такой антивирус?

Наличие песочницы[14]

Под песочницей (sundbox) в данном случае понимают программную песочницу - изолированную среду исполнения с контролируемыми правами. То есть суть антивирусных песочниц - защита основной рабочей системы от потенциально опасного контента.

Можно выделить ***три базовые модели изоляции пространства песочницы от всей остальной системы***.

Изоляция на основе полной виртуализации. Использование любой виртуальной машины в качестве защитного слоя над гостевой операционной системой, где установлен браузер и иные потенциально опасные программы, через которые пользователь может заразиться, даёт достаточно высокий уровень защиты основной рабочей системы.

Недостатки подобного подхода, кроме монструозного размера дистрибутива и сильного потребления ресурсов, кроются в неудобствах обмена данными между основной системой и песочницей. Более того, нужно постоянно возвращать состояние файловой системы и реестра к исходным для удаления заражения из песочницы. Если этого не делать, то, например, агенты спам-ботов будут продолжать свою работу внутри песочницы как ни в чём не бывало.

Пример подхода- Invincea.

Организовать такую песочницу администратор может самостоятельно на базе какой-либо виртуальной машины. Например, VirtualBox. Это имеет смысл если нужно открывать какие-либо подозрительные ресурсы.

Изоляция на основе частичной виртуализации файловой системы и реестра. Совсем необязательно таскать с собой движок виртуальной машины, можно подпихивать процессам в песочнице дубликаты объектов файловой системы и реестра, помещая в песочницу приложения на рабочей машине пользователя. Попытка модификации данных объектов приведёт к изменению лишь их копий внутри песочницы, реальные данные не пострадают. Контроль прав не даёт возможности атаковать основную систему изнутри песочницы через интерфейсы операционной системы.

Недостатки подобного подхода также очевидны– обмен данными между виртуальным и реальным окружением затруднён, необходима постоянная очистка контейнеров виртуализации для возврата песочницы к изначальному, незаражённому состоянию. Также, возможны пробои либо обход такого вида песочниц и выход

[14] https://habrahabr.ru/post/105581/

зловредных программных кодов в основную, незащищённую систему.

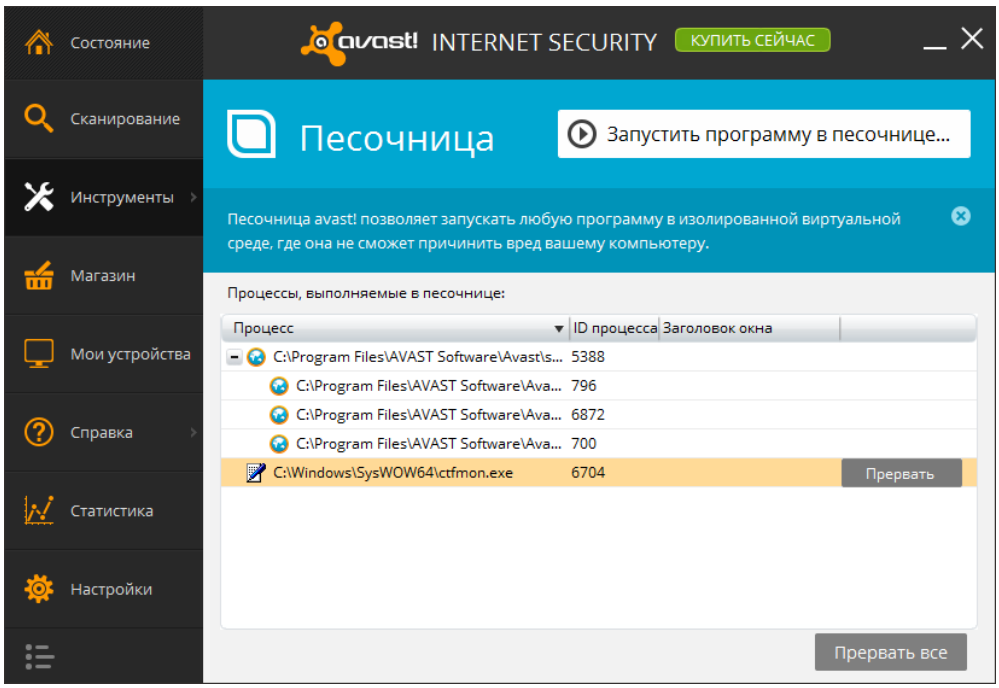

Рисунок 22 Настройки песочницы Avast

Пример подхода- SandboxIE, BufferZone, ZoneAlarm ForceField, изолированная среда Kaspersky Internet Security, Comodo Internet Security sandbox, Avast Internet Security sandbox.

Изоляция на основе правил. Все попытки изменения объектов файловой системы и реестра не виртуализируются, но рассматриваются с точки зрения набора внутренних правил средства защиты. Чем полнее и точнее такой набор, тем большую защиту от заражения основной системы предоставляет программа. То есть, этот подход представляет собой некий компромисс между удобством обмена данными между процессами внутри песочницы и реальной системой и уровнем защиты от зловредных модификаций. Контроль прав не даёт возможности атаковать основную систему изнутри песочницы через интерфейсы операционной системы.

К плюсам такого подхода относится, также, отсутствие необходимости постоянного отката файловой системы и реестра к изначальному состоянию.

Недостатки подобного подхода– программная сложность реализации максимально точного и полноценного набора правил, возможность лишь частичного отката изменений внутри песочницы. Так же, как и любая песочница, работающая на базе рабочей системы, возможен пробой либо обход защищённой среды и выход зловредных кодов в основную, незащищённую среду исполнения.

Пример подхода- DefenseWall, Windows Software Restriction Policy, Limited User Account + ACL.

Существуют и смешанные подходы к изоляции процессов песочницы от остальной системы, основанные как на правилах, так и на виртуализации. Они наследуют как достоинства обоих методов, так и недостатки. Причём недостатки превалируют из-за особенностей психологического восприятия пользователей.

Примеры подхода- GeSWall, Windows User Account Control (UAC).

Существует ***три метода определения нужно ли помещать процесс в песочницу***:

На основе правил. То есть, модуль принятия решения смотрит на внутреннюю базу правил запуска тех или иных приложений или потенциально опасных файлов и, в зависимости от этого, запускает процессы в песочнице либо вне неё, на основной системе.

Преимущества данного подхода- наиболее максимальный уровень защиты. Закрываются как зловредные программные файлы, пришедшие из потенциально опасных мест через песочницу, так и неисполняемые файлы, содержащие зловредные скрипты.

Недостатки– могут быть проблемы при установке программ, пришедших через песочницу (хотя белые списки и сильно облегчают эту задачу), необходимость вручную запускать процессы в основной, доверенной зоне для обновления программ, обновляющихся только внутри себя самих (например, Mozilla FireFox, Utorrent или Opera).

Примеры программ с таким подходом- DefenseWall, SandboxIE, BufferZone, GeSWall.

На основе прав пользователя. Так работает Windows Limited User Account и защита на основе SRP и ACL. При создании нового пользователя ему предоставляются права доступа к определённым ресурсам, а также ограничения на доступ к другим. При необходимости программы работы с запрещёнными для данного пользователя ресурсами необходимо либо перелогиниться в системе под пользователем с подходящим набором прав и запустить программу, либо запустить её одну под таким пользователем, без перелогинивания основного работающего пользователя (Fast User Switch).

Преимущества такого подхода- относительно неплохой уровень общей защищённости системы.

Недостатки- нетривиальность управления защитой, возможность заражения через разрешённые для модификации ресурсы, поскольку модуль принятия решения не отслеживает такие изменения.

На основе эвристических подходов. В этом случае модуль принятия решения «смотрит» на исполняемый файл и пытается по косвенным данным угадать, запустить его на основной системе или в песочнице. Примеры– Kaspersky Internet Security HIPS, Comodo Internet Security sandbox.

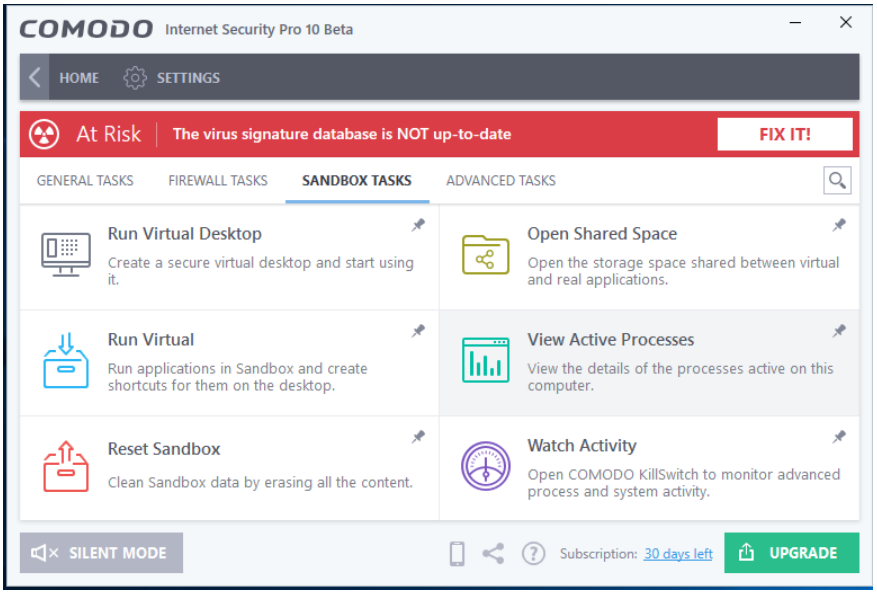

Рисунок 23 Настройки Comodo sandbox

Преимущества данного подхода- он более прозрачен для пользователя, чем на основе правил. Проще в обслуживании и реализации для компании–производителя.

Недостатки- неполноценность подобной защиты. Кроме того, что эвристик модуля принятия решения может «промахнуться» на исполняемом модуле, такие решения демонстрируют практически нулевую сопротивляемость неисполняемым файлам, содержащим зловредные скрипты. Ну, плюс ещё парочка проблем (например, с установкой зловредных расширений изнутри самого браузера, из тела эксплойта).

Есть всего два основных режима использования песочниц:.

Режим постоянной защиты. При старте процесса, который может быть угрозой для основной системы, он автоматически помещается в песочницу.

Режим ручной защиты. Пользователь самостоятельно принимает решение о запуске того либо иного приложения внутри песочницы.

Дополнительные функции

Антивирусное ПО может обладать дополнительными функциями. Они могут быть напрямую связаны с основной задачей:

- файрволл/брандмауэр;
- песочница для выполнения безопасных платежей.

Или просто относится каким то образом к обеспечению безопасной работы системы:

менеджер паролей;

родительский контроль;

механизм слежения за обновлениями программ.

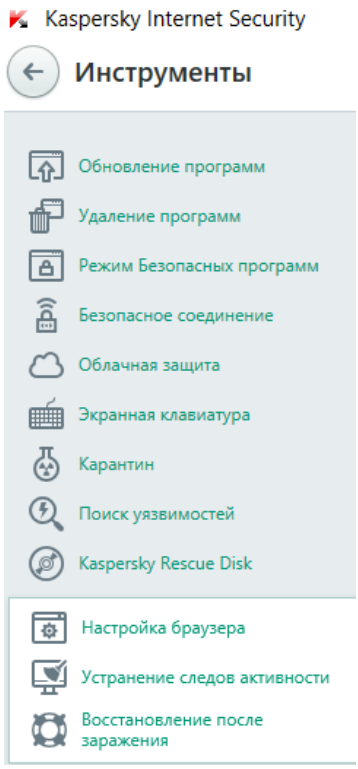

Рисунок 24 Дополнительные функции KIS

Список дополнительных функций может быть очень большим. ***Задача состоит в том, чтобы определится насколько эти функции необходимы.*** Не стоит забывать про качество их реализации. Немаловажным является тот факт, что ***предоставляемый набор функций зависит от выбранного варианта схемы лицензирования, а значит от цены.***

Стоимость и схема лицензирования

Существует как платное так и бесплатное антивирусное ПО. Конечно, прямой зависимости между качеством работы программы и ее стоимостью нет. Но, как уже говорилось выше у фирм, продающих программы за деньги больше скорость внесения изменений в антивирусные базы, и , часто более качественно отлажены алгоритмы и их реализации. Тем не менее ***НЕЛЬЗЯ сказать, что платное ПО однозначно хорошо а бесплатное антивирусное ПО- плохо. Это не так!***

Нужно учитывать, что ***подавляющее большинство бесплатных версий антивирусных программ по условиям их лицензии могут использоваться только дома и в некоммерческих целях***. Конечно, условия отличаются, но в целом картина такова - бесплатные антивирусы только для дома. Исключением в 2017 году является 360 Total Security, AVZ, Clam и некоторые другие. Частично бесплатной можно считать Microsoft Security Essentials которая бесплатна для дома и организаций если в них меньше 10 компьютеров и это не учреждения образования и гос. учреждения.

Поэтому ***первое в чем стоит убедится выбирая бесплатную антивирусную программу - является ли она бесплатной в данных условиях, данной организации.***

Отмечу также, что все известные мне бесплатные антивирусные программы, кроме Clam, активно предлагают пользователю купить платную версию (например Avast) или монетизируются за счет показа рекламного контента (360 Total Security). Встречаются варианты, когда при обнаружении вируса программа предлагает для лечения купить полноценную версию

Поэтому ***второе на что стоит обратить внимание - схема монетизации бесплатного антивируса.***

Платные антивирусы используют схемы лицензирования по которым, для того чтобы сохранить возможность обновления антивирусных баз и самой программы, нужно приобретать продление лицензии. Обычно период продления - год.

Понятно, что без таких обновлений уровень защиты непрерывно снижается.

Определяя стоимость приобретения антивируса нужно учитывать не только начальную цену но и сколько будет стоить продление в течении срока использования.

Например Kaspersky Internet Security для домашнего использования на 2 устройства стоит 1990 р. А продление на год 1490. Значит за три года, даже если цена не изменится, стоимость составит 1990+3*1490=6460 р.

Также цена может отличаться для юридических лиц и для физических лиц.

Многие компании предоставляют скидки для различных групп покупателей. Например Kaspersky предоставляет скидку до 80% для образовательных организаций.

Симптомы заражения

Существует ряд признаков, свидетельствующих о заражении компьютера[15].

Основные симптомы:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- неожиданно открывается и закрывается лоток CD-ROM-устройства;
- произвольно, без участия пользователя, запускаются какие-либо программы;
- запускаются подозрительные процессы

[15] https://support.kaspersky.ru/790

- в списке автозагрузки и планировщике появляются неизвестные записи
- на экран выводятся предупреждения о попытке какой-либо из программ выйти в интернет, хотя пользователь никак не инициировал такое ее поведение,
- при переходе на сайты открываются страницы с рекламой или угрозами.
- в содержимое страниц открываемых в браузере встраиваются дополнительные рекламные блоки.
- в почтовом ящике пользователя находится большое количество сообщений без обратного адреса и заголовка.
- друзья или знакомые говорят пользователю о сообщениях от него через e-mail, мессенджеры, социальные сети которые он не отправлял;
- происходят непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- удаляются файлы или появляются новые без ведома пользователя
- становится невозможно сохранять файлы в нужных каталогах;
- появляются ошибки при загрузке операционной системы;
- становится невозможно войти в систему.

Наличие перечисленных признаков, с большой степенью вероятности, означает что компьютер поражен вирусом.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с обратным адресом пользователя, но не с его компьютера.

Существуют также косвенные симптомы заражения компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- браузер "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении.

Заболел - лечись!

Если компьютер заражен вирусом, то дальнейшие действия завися от типа вируса и того, как он заражает систему.

Если есть возможность нужно в первую очередь сделать резервную копию важных данных. Лучше всего для этого загрузится с какого-либо LiveCD или Linux Live USB. Загрузка с Windows Live USB может привести к его заражению.

Если в результате лечения часть данных будет утеряна можно будет использовать полученную копию как источник для лечения зараженных файлов другими утилитами.

Если лечение пройдет успешно – сделанную перед лечением резервную копию нужно удалить. Для восстановления данных ее использовать нельзя, так как файлы в ней заражены.

Вход в систему возможен.

Провести полную проверку системы при помощи имеющегося антивирусного ПО. Данное действие нужно выполнить как самое простое, но вероятность того, что оно поможет невысока, так как если система заражена – значит данный антивирус не справился.

Провести полную проверку при помощи другого антивирусного ПО. Бывают ситуации, когда вирус детектируется не всеми антивирусами. Поэтому нужно проводить проверку программами разных фирм. Если в системе уже есть антивирус – нужно предварительно отключить его монитор. Иначе модули сканирования и мониторы разных антивирусов будут конфликтовать, и система зависнет.

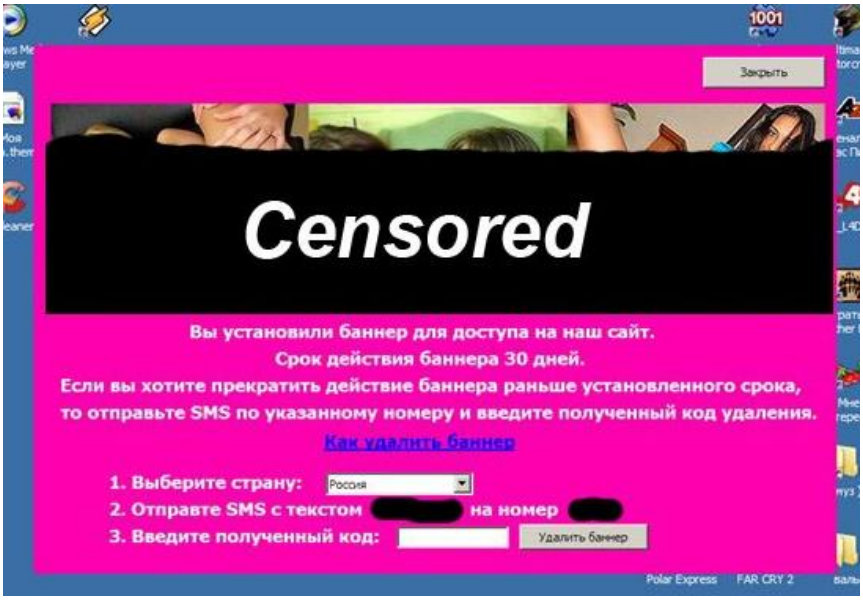

Рисунок 25 Окно вируса-блокировщика

Для такой проверки можно использовать бесплатные модули проверки, например, DrWeb CureIt! или Kaspersky Virus Removal Tool. Эти программы не требуют установки, но используют то же ядро, базы и алгоритмы что и полные версии.

Проверить список запущенных процессов. Вирус может отображаться в списке запущенных процессов. Следует проверить все процессы, назначение которых неизвестно или поведение вызывает подозрение.

Если в результате работы вируса на экран выводятся сообщения/рекламные баннеры, то можно попробовать определить создавший их процесс с помощью утилиты Process Explorer.

Для всех подозрительных процессов можно узнать «место хранения файла» и по найденному файлу выяснить природу заражения.

Если найден вредоносный процесс его нужно остановить, а затем завершить. Но это временное решение. Процесс может быть перезапущен. Нужно искать как его удалить из системы.

Воспользоваться точкой восстановления системы.

Браузер всегда открывает одну и ту же страницу с рекламой/угрозами.

Выполнить предыдущие шаги по лечению системы, а затем **проверить следующие настройки.**

Настройки прокси в свойствах браузера

Настройки IP сервера DNS

Содержимое файла hosts

Наличие и настройки туннельных драйверов, например Teredo

Браузер открывает дополнительные страницы с рекламой. В открываемые страницы встраиваются «лишние» блоки рекламы

То, что рекламные блоки встроены на стороне клиента можно проверить, перейдя на страницу, на которой таких блоков быть не должно. Например google.com или ya.ru Наличие рекламы на этих страницах или появление дополнительных страниц с рекламой при переходе на эти страницы говорит о заражении ad-ware программами.

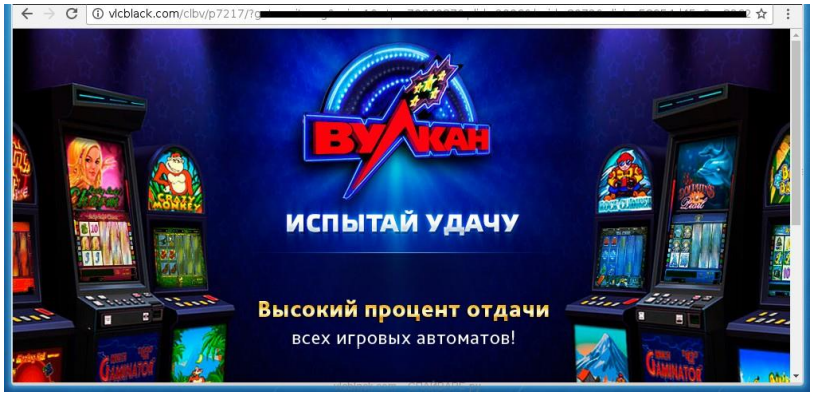

Рисунок 26 Пример рекламного окна

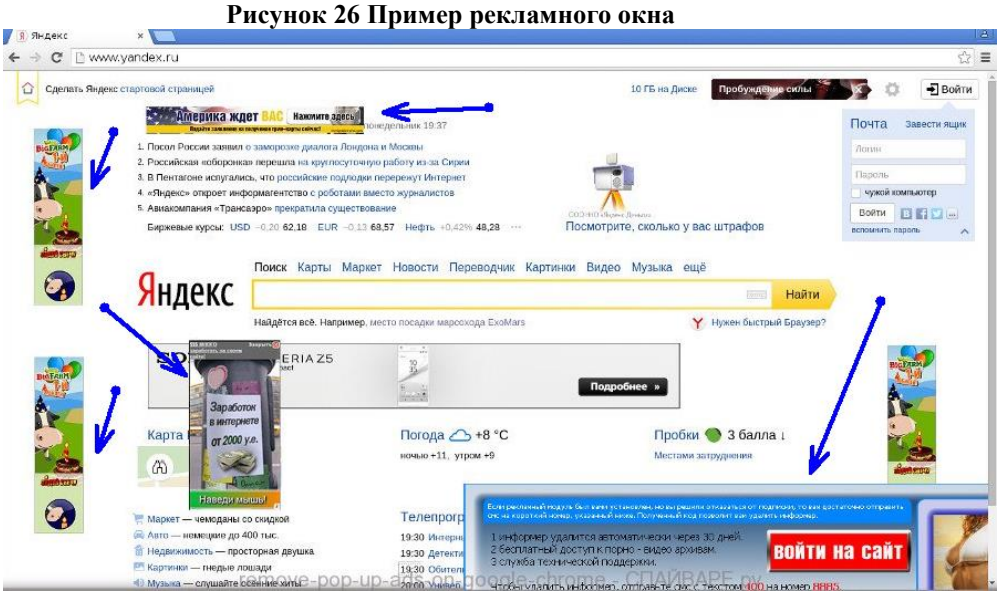

Рисунок 27 Лишние баннеры на странице Yandex

Можно выполнить предыдущие шаги по лечению системы, но нужно помнить, что формально это не вирус и часто антивирусное ПО их игнорирует.

Можно **проверить какие расширения установлены в браузере и каковы настройки прокси сервера**.

Можно **воспользоваться специальной программой**, например, бесплатным ПО от Malwarebytes.

Проблемы возникают только у одного из пользователей. При работе появляется экран с сообщением о блокировке.

Заражен только профиль пользователя.

Попробовать обойти экран блокировки при помощи Ctrl+Alt+Del – завершить процесс или перезапустить explorer.exe. Если экран блокирует рабочий стол можно нажать «Файл» – «Выполнить» в Диспетчере задач и нажав «Обзор» получить доступ к файловой системе.

Можно **создать нового пользователя с чистым профилем**. Если проблема проявится и там – заражен профиль DefaultUser

Нужно зайти от имени администратора и выполнить поиск и удаление всех файлов, кроме документов созданных пользователем, которые были созданы или изменены в период заражения или в течении суток до этого.

Нельзя выполнить вход в систему. Система не запускается. В момент входа появляется сообщение о блокировке.

Проверить систему при помощи антивируса запустив его с загрузочного носителя.

Например, можно воспользоваться Dr.Web LiveDisk или Kaspersky Rescue Disk. Эти дистрибутивы основаны на Linux и в достаточной степени защищены от заражения. В них встроены утилиты сканирования и лечения, а также браузер и средства обновления антивирусных баз.

Более опасным является подключение зараженного накопителя/жесткого диска к рабочей системе с целью проверки. В этом случае велик риск заражения второй системы. И разумно использовать компьютер на базе Linux с запущенным на нем Clam или т.п. ПО.

Воспользоваться точкой восстановления системы.

Список источников

1. Microsoft FAQ Defining Malware: FAQ - http://technet.microsoft.com/en-us/library/dd632948.aspx
2. Microsoft Malware Protection Center Worm:Win32/Morto.A - http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Morto.A
3. Windows-компьютер без антивирусов - http://habrahabr.ru/post/97594/
4. Анализ и лечение классических вирусов - http://www.nobunkum.ru/ru/file-infectors
5. Аналитический отчет по безопасности Майкрософт, Том 14 (Июль декабрь 2012) - http://www.microsoft.com/ru-ru/download/details.aspx?id=38433
6. Как бороться с сетевым червем Net-Worm.Win32.Kido - http://support.kaspersky.ru/viruses/disinfection/1956#block0
7. Касперски К. Компьютерные вирусы изнутри и снаружи – Спб: Питер, 2010. -526 с. - ISBN 5-469-00982-3
8. Касперский. Азбука безопасности - http://www.kaspersky.ru/threats_faq
9. Климентьев К. Компьютерные вирусы и антивирусы. Взгляд программиста – М.: «ДМК Пресс», 2013. – 656 с. - ISBN 978-5-94074-885-4
10. Немет Э., Снайдер Г., Хейн Трент Р., Уэйли Б. Unix и Linux. Руководство системного администратора. – М.: Вильямс, 2012. – 1312 с. - ISBN 978-5-8459-1740-9
11. Обманчивая безопасность RTF-файлов - http://www.kaspersky.ru/about/news/virus/2001/Obmanchivaya_bezopasnost_RTF-failov