Содержание

Введение

Проект помогает разобраться:

- в видах вирусов, особенностях их распространения и лечения;

- в большом количестве предлагаемых антивирусных программ и частично в подборе наилучшей защиты

- помогает понять что такое web-страница и web-сайт

- как они создаются и каких видов бывают

Цели проекта:

- приобретение опыта использования информационных технологий в индивидуальной и коллективной учебной и познавательной;

- воспитание ответственного отношения к соблюдению этических и правовых норм информационной деятельности;

- развитие познавательных интересов, интеллектуальных и творческих способностей;

- овладение умениями применять, анализировать, преобразовывать информацию

В результате изучения темы проекта ученик должен:

знать:

- основные технологии создания, редактирования, оформления, сохранения, передачи информационных объектов различного типа с помощью современных программных средств информационных и коммуникационных технологий.

уметь:

- оперировать различными видами информационных объектов, в том числе с помощью компьютера, соотносить полученные результаты с реальными объектами;

- оценивать достоверность информации, сопоставляя различные источники;

- иллюстрировать учебные работы с использованием средств информационных технологий;

- создавать информационные объекты сложной структуры, в том числе гипертекстовые документы;

- соблюдать правила техники безопасности и гигиенические рекомендации при использовании средств ИКТ.

использовать приобретенные знания и умения в практической деятельности и повседневной жизни для:

- эффективного применения информационных образовательных ресурсов в учебной деятельности, в том числе самообразовании;

- ориентации в информационном пространстве, работы с распространенными автоматизированными информационными системами;

- автоматизации коммуникационной деятельности;

- соблюдения этических и правовых норм при работе с информацией;

- эффективной организации индивидуального информационного пространства.

Вопросы, ведущие проекта

Проблемные вопросы

Как распространяется вирус и что это такое?

Какие вирус наиболее опасен?

Как выбрать антивирусную программу?

Как создать Web-страницу?

Учебные вопросы

Что такое компьютерный вирус?

Каковы механизм и каналы распространения вирусов?

Какие могут быть возможности противодействия компьютерным вирусам?

Какие антивирусы существуют на данный момент?

Какие антивирусные средства наиболее эффективны?

Каких видов бывают Web-страницы?

Что понимается под Web-страницей и Web-сайтом?

Компьютерные вирусы и их методы классификации

Компьютерный вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных.

Известно много различных способов классификации компьютерных вирусов.

Одним из способов классификации компьютерных вирусов – это разделение их по следующим основным признакам:

- среда обитания;
- особенности алгоритма;
- способы заражения;
- степень воздействия (безвредные, опасные, очень опасные).

В зависимости от среды обитания основными типами компьютерных вирусов являются:

1. Программные (поражают файлы с расширением. COM и .EXE) вирусы.
2. Загрузочные вирусы.
3. Макровирусы.
4. Сетевые вирусы.

Программные вирусы – это вредоносный программный код, который внедрен внутрь исполняемых файлов (программ). Вирусный код может воспроизводить себя в теле других программ – этот процесс называется размножением.

По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удаляя информации, хранящиеся на жестком диске. Этот процесс называется вирусной атакой.

Загрузочные вирусы – поражают не программные файлы, а загрузочный сектор магнитных носителей (гибких и жестких дисков).

Макровирусы – поражают документы, которые созданы в прикладных программах, имеющих средства для исполнения макрокоманд. К таким документам относятся документы текстового процессора WORD, табличного процессора Excel. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

Сетевые вирусы пересылаются с компьютера на компьютер, используя для своего распространения компьютерные сети, электронную почту и другие каналы.

По алгоритмам работы различают компьютерные вирусы:

- черви (пересылаются с компьютера на компьютер через компьютерные сети, электронную почту и другие каналы);
- вирусы-невидимки (Стелс-вирусы);
- троянские программы;
- программы – мутанты;
- логические бомбы;
- и другие вирусы.

В настоящее время к наиболее распространенным видам вредоносных программ, относятся: черви, вирусы, троянские программы.

Интересный факт:

Первая массовая эпидемия компьютерного вируса произошла в 1986 году, когда вирус «Brain» «заражал» дискеты для первых массовых персональных компьютеров, заражены были более 18000 компьютеров. Один из самых опасных из всех известных вирусов Интернета – вирус «Чернобыль». Вирус активизируется 26 апреля, но модификации могут принести вред и 26 числа каждого месяца, кроме порчи информации на диске он перепрограммирует систему загрузки компьютера и компьютер перестает загружаться.

Вирус «Я люблю тебя» филиппинского происхождения, распространялся по электронной почте. Он вывел из строя 45 млн. компьютеров во всем мире. Основная атака произошла 4 мая 2000г. Вирус уничтожал графические и звуковые файлы. Материальный ущерб составил около 10 млрд. долларов

Признаки заражения ПК вирусом

Желательно не допускать появление вирусов в ПК, но при заражении компьютера вирусом очень важно его обнаружить.

Основные признаки появления вируса в ПК:

- медленная работа компьютера;
- зависания и сбои в работе компьютера;
- изменение размеров файлов;
- уменьшение размера свободной оперативной памяти;
- значительное увеличение количества файлов на диске;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов.

Способы защиты от компьютерных вирусов

Одним из основных способов борьбы с вирусами является своевременная профилактика.

Чтобы предотвратить заражение вирусами и атаки троянских коней, необходимо выполнять некоторые рекомендации:

- Не запускайте программы, полученные из Интернета или в виде вложения в сообщение электронной почты без проверки на наличие в них вируса.

- Необходимо проверять все внешние диски на наличие вирусов, прежде чем копировать или открывать содержащиеся на них файлы или выполнять загрузку компьютера с таких дисков.

- Необходимо установить антивирусную программу и регулярно пользоваться ею для проверки компьютеров. Оперативно пополняйте базу данных антивирусной программы набором файлов сигнатур вирусов, как только появляются новые сигнатуры.

- Необходимо регулярно сканировать жесткие диски в поисках вирусов. Сканирование обычно выполняется автоматически при каждом включении ПК и при размещении внешнего диска в считывающем устройстве. При сканировании антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящихся в базе данных.

- создавать надежные пароли, чтобы вирусы не могли легко подобрать пароль и получить разрешения администратора. Регулярное архивирование файлов позволит минимизировать ущерб от вирусной атаки

- основным средством защиты информации – это резервное копирование ценных данных, которые хранятся на жестких дисках

Существует достаточно много программных средств антивирусной защиты. *Современные антивирусные программы состоят из модулей:*

- Эвристический модуль – для выявления неизвестных вирусов.

- Монитор – программа, которая постоянно находится в оперативной памяти ПК

- Устройство управления, которое осуществляет запуск антивирусных программ и обновление вирусной базы данных и компонентов

- Почтовая программа (проверяет электронную почту)

- Программа сканер – проверяет, обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системных областях дисков

- Сетевой экран – защита от хакерских атак

Но самым главным является Антивирусная программа

Антивирусная программа

Антивирус – это программа для защиты компьютера или мобильного устройства от вредоносных программ. Термин «вредоносные программы» включает в себя все

возможные виды опасных программ, таких, как вирусы, черви, трояны и вирусы-шпион

Эффективность антивирусов

Сразу стоит сказать, что нет идеального антивируса. Да, антивирусы защищают компьютер, но ни один антивирус не защитит ваш компьютер на все 100%. Почему? Дело в том, что суть работы антивируса заключается в его алгоритмах, благодаря которым распознаётся наличие вирусов в компьютере. Обнаружение вирусов происходит по их активности или по определённым действиям. Когда антивирусу известен вирус и его особенности, то, при его попадании в компьютер, антивирус замечает его и информирует пользователя об опасности. Это то, что касается известных антивирусов, но также есть и новые вирусы, которые пока не известны разработчикам антивирусов и не внесены в антивирусные базы. Такая ситуация также продумана. Для этого алгоритмы антивируса контролируют активность файлов и приложений и при их подозрительных действиях информируют пользователя, предлагая определённый перечень действий. Всё это хорошо, но существуют вирусы, которые антивирус может не заметить, это, как правило, новые вирусы либо же обновлённые старые. Есть и другие причины пропуска антивирусом вирусов, но их мы затрагивать, пожалуй, не будем.

Защита компьютера в Интернете

Современные антивирусные программы включают в себя не только возможность обнаружения и удаления вирусов, но также возможность осуществлять защиту компьютера от различных нежелательных последствий: хакерской атаки, навязчивой рекламы на сайтах, спама и т.п. Таким образом, антивирус включает в себя файрвол, о котором, наверное, большинство из вас слышали. Если раньше антивирус и файрвол были разными программами, то сейчас, как правило, самые лучшие и продвинутые версии антивирусов включают в себя комплексную защиту, то есть антивирус+файрвол

По каким критериям выбрать лучший антивирус

Лучший антивирус для собственного компьютера изначально должен включать в себя базовые функции и иметь особенности, которые мы перечислим ниже:

- Антивирусный сканер. Функция сканера производит сканирование жёсткого диска и оперативной памяти для поиска в них вирусов. Очень хорошо, если периодически сканер будет в автоматическом режиме проверять изменившиеся и добавленные файлы, для так называемой пассивной безопасности.
- Антивирусный монитор. Данная функция антивируса осуществляет непрерывный контроль деятельности вашего компьютера, то есть он мониторит все

события, которые происходят на компьютере, не давая просочиться в компьютер вирусам.

- Контроль программ. Достаточно часто вирусы проникают в программы или являются псевдопрограммой, именно для этого создана функция контроля программ. При наличии каких-либо подозрительных действий программ данный контроль сразу же сообщает об этом пользователя и определяет тип угрозы.
- Контроль сети и веб-антивирус. Ещё одна необходимая на наш взгляд функция антивируса заключается в контроле локальной сети и Интернет-трафика. Таким образом, вы будете защищены от атаки компьютера из локальной сети и Интернета, а также от негативных последствий вредоносных кодов и зараженных сайтов.
- Возможность гибких настроек. Чем больше настроек имеет антивирус, тем лучше. Благодаря этому вы сможете выбрать уровень контроля той или иной функции антивируса: низкий, средний или высокий, либо же вовсе отключить ненужные функции для того, чтобы убрать лишнюю загрузку ресурсов своего компьютера. Кроме того, вы сможете создать свои правила поиска и обнаружения вирусов, а также предпринимаемых антивирусом действий при определении вирусной активности на вашем компьютере.
- Обновление антивирусных баз. Антивирусные базы – это так называемая картотека вирусов и хранилище алгоритмов для их обнаружения и нейтрализации. Для надёжной защиты компьютера антивирусные базы должны постоянно обновляться и быть актуальными, благодаря чему, при появлении в сети нового вируса, разработчики создадут алгоритм нейтрализации и внесут его в антивирусную базу. При частом обновлении антивирусных баз ваш антивирус будет иметь самые свежие алгоритмы для нейтрализации новых или обновлённых вирусов.
- Самозащита антивируса. Антивирус должен обеспечивать не только безопасность компьютера, но и свою собственную безопасность. То есть, антивирус должен иметь самозащиту, благодаря которой вирусы не смогут его отключить, нейтрализовать или заблокировать запуск. Это является ещё одной причиной, по которой антивирус может не обнаружить или не удалить вирус.
- Рациональное потребление ресурсов в пассивном режиме. Ну и последний немаловажный фактор при выборе антивируса - необходимо проанализировать потребление им ресурсов компьютера. Несмотря на то, что современные антивирусы экономно используют ресурсы компьютера при работе в пассивном режиме, тем не менее, некоторые неудачные версии антивирусов могут

иметь такую проблему, поэтому нужно обратить на это внимание. Следует отметить, что нужно отличать пассивный режим работы антивируса и активный. Пассивный режим – это когда антивирус свёрнут в трей и мониторит работу компьютера, а активный – когда вы самостоятельно запустили проверку компьютера на вирусы или производите другое активное действие.

Это так называемые базовые функции, которые должны обязательно быть в вашем антивирусе. Исключение может составлять лишь контроль сети, который относится к файрволу.

Какой антивирус самый лучший?

У всех юзеров есть свои критерии и предпочтения в антивирусах, именно поэтому у каждого пользователя будет свой лучший антивирус. Перед тем как коснуться списка лучших антивирусов, по мнению экспертов сайта MasterServis24.ru, стоит сказать, что подавляющее большинство антивирусов имеют 2 вида антивирусных программ для компьютеров и ноутбуков: простой антивирус и антивирус-файрвол (с наличием дополнительных функций). Для домашнего компьютера вполне хватит обычного антивируса, но если говорить в ключе нашей темы, то лучшим можно назвать дистрибутив, который включает в себя антивирус-файрвол. Если на вашем компьютере нет Интернет-подключения, то, по сути, версия со встроенным файрволом вам не нужна, если же у вас есть доступ в Интернет, то рекомендуем установить антивирус с файрволом.

Заражение веб-сайта

Заражение веб-сайта проводится через дефекты безопасности в коде веб-приложений и изъяны конфигурации компонентов, которые позволяют киберпреступникам выполнить взлом и внедрить вредоносный код.

Современный бизнес неразрывно связан с использованием веб-технологий. Для крупных компаний разрабатываются целые порталы, которые по сути являются наборами приложений и используются в деловых либо производственных процессах. Но как только доступ к ним становится возможным через интернет, они оказываются лакомой целью для киберпреступников. Чаще всего атаки на сайты проводят через уязвимости их компонентов.

Никогда нельзя сказать с уверенностью, заражен ли открытый в браузере сайт. Инфицированными могут оказаться как заведомо опасные сайты («варез», торренты), так и популярные и полностью легальные ресурсы.

Классификация способов заражения веб-сайта

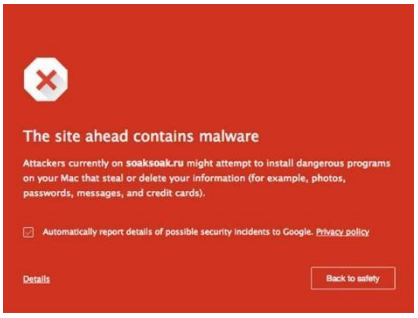
1. Заражение через FTP. Многие вебмастера для работы с сайтом через FTP используют файловые менеджеры, которые сохраняют пароли и логины для автоматической авторизации. Часто такие данные хранятся в незашифрованном виде, и при заражении компьютера вредоносной программой они могут попасть к злоумышленникам.
2. Некоторые системы управления сайтом (CMS) не обладают защитой от брутфорс-атаки. В них не предусмотрены проверки CAPTCHA, ограничение количества попыток ввода паролей. Если при этом используется стандартный логин (Admin или Administrator) и пароль, состоящий из одних цифр, то взлом и заражение веб-сайта значительно упрощаются.
3. Открытые уязвимости в CMS также могут предоставить злоумышленнику несанкционированный доступ. Это возможно в том случае, если используется устаревшая версия системы управления сайтом.
4. Вебмастера, создавая и развивая сайт, сталкиваются с необходимостью приобретения платных модулей, компонентов и плагинов. Стоимость их может быть высокой, и вполне закономерно стремление найти взломанные бесплатные варианты. Киберпреступники, зная о желании вебмастеров сэкономить, публикуют такие версии со встроенным вредоносным кодом, с помощью которого сайт будет заражен или открыт для удаленного администрирования.

Источник угрозы

Вредоносные программы используются злоумышленниками для достижения определенных целей:

- Внедрение эксплойтов для последующей скрытой инсталляции потенциально опасных программ посетителям и клиентам сайта.
- Переадресация трафика на рекламные модули, шпионский, фишинговый и прочий нежелательный контент.
- Перехват и присваивание посещений при вводе определенных поисковых запросов.
- Продвижение веб-адресов с сомнительным содержимым (такое явление называется черной оптимизацией).
- Применение возможностей сервера для незаконной активности, например проведения DDoS-атак.

Любые действия нечестных разработчиков направлены на получение прибыли. Методы могут сильно отличаться: от перехвата потоков трафика для накрутки количества посещений до похищения ключей от электронных кошельков и прочей конфиденциальной информации.



Особая опасность заражения сайтов состоит в том, что оно часто оказывается незаметным для администратора. Владельцы сайта могут не подозревать о проблеме, так как вредоносный код будет отдаваться по настроенному таргетингу (для определенного региона, в определенное время, на определенной платформе).

Как происходит заражение веб-сайта?

Самый простой способ — взлом пароля путем перебора или словарной атаки. Эта тактика занимает много времени и является неэффективной, поэтому при массовых заражениях она употребляется крайне редко. Гораздо чаще используются уязвимости системы управления контентом или специальное программное обеспечение для похищения паролей.

Большинство современных CMS-платформ далеко от совершенства, в них содержится множество уязвимостей, благодаря которым сторонние лица могут загружать любую информацию. Разработчики регулярно тестируют собственные продукты на наличие неполадок, но выход обновлений с обнаруженными и исправленными ошибками обычно происходит далеко не сразу, а многие люди пользуются еще более старыми версиями, в которых может быть множество багов. Неудивительно, что уязвимости часто встречаются в распространенных платформах WordPress, Joomla и подобных им.

Квалифицированные киберпреступники предоставляют вебмастерам возможность самостоятельно заразить свой сайт. Такое событие возможно, когда злоумышленники выкладывают в общий доступ полезные CMS-модули с вредоносной начинкой, которые вебмастер скачивает и добавляет на сайт, тем самым инфицируя его.

В некоторых случаях злоумышленники пользовались другим методом. Сначала распространялось программное обеспечение, предназначенное для поиска и несанкционированного копирования данных FTP-аккаунтов посредством внесения изменений в клиентские службы или путем сканирования сетевого трафика. Затем

приложения соединялись с командным сервером и загружали заранее подготовленные скрипты или измененные версии оригинального контента. Это приводило к повторному заражению однажды инфицированного компьютера даже после изменения регистрационной информации, отката к предыдущему состоянию или восстановления из заранее созданной резервной копии.

Подводя итог вышесказанному, можно прийти к выводу, что заражение может быть произведено одним из следующих способов:

- Вредоносный код преднамеренно был размещен владельцем для получения незаконной прибыли или иных целей.
- Сайт был взломан, и фрагмент с потенциально опасным содержимым был размещен на нем посторонними хакерами; сегодня это — один из самых распространенных вариантов.
- Нежелательный объект содержится не на самом сайте, а в коде внешнего контента, размещенного на странице. В этом случае атака идет не напрямую, а через баннерную сеть, виджеты или другие подобные компоненты; инфекция распространяется через все сайты, чьи страницы содержат ссылку на зараженный объект.

Анализ риска

Как показывают исследования, риск посетить инфицированный сайт весьма велик. При этом заражение может произойти незаметно. Особенно велика вероятность приобрести нежелательных «пассажиров» в следующих случаях:

- использование для серфинга и другой деятельности в Интернете компьютера с уязвимым программным обеспечением;
- постоянное и повседневное использование учетной записи администратора;
- выбор примитивных паролей, которые легко взламываются;
- несвоевременное обновление защитных решений.

Последствия могут быть самыми разнообразными: от постоянного получения спама и прочих подобных сообщений до потери контроля над учетными записями в соцсетях или значительной части денежных средств.

При обнаружении симптомов нужно деактивировать сайт, предотвращая дальнейшее распространение вредоносной нагрузки. Затем следует проверить серверные журналы на наличие следов несанкционированной активности. Это может помочь определить инфицированные компоненты и возможные пути их появления.

Для полного восстановления содержимого сервера устанавливаются созданная до инфицирования резервная копия и последние версии всех программ, предназначенных для работы с оборудованием.

Если чистой копии нет, необходимо использовать автоматизированные средства для выявления потенциально опасных записей. Подобную опцию содержат многие антивирусные продукты, также для этих целей разработаны специализированные онлайн-сканеры. Для более тщательной проверки можно поочередно использовать несколько таких решений, часть из которых определит уровень угрозы и укажет на содержащие подозрительные записи фрагменты. После этого проводится антивирусное сканирование всех размещенных на сервере файлов.

Владельцы серверов могут выполнить их комплексную проверку. Содержимое загружается на локальную машину и проверяется антивирусом со встроенным эвристическим модулем. Второй способ показывает более высокие результаты при борьбе с подобными угрозами.

Если проверка в автоматическом режиме не принесла результатов, можно попробовать найти и удалить вредоносное содержимое вручную. Это — весьма трудоемкий процесс, в ходе которого предстоит проверить каждый файл на наличие посторонних скриптов. Особое внимание следует уделить неясным или нечитаемым фрагментам. Обфускация кода нетипична для используемого в сайтостроении ПО. При обнаружении ее малейших признаков необходимо все тщательно проверить. Аналогично выявляются ссылки на внешние ресурсы.

Для профилактики заражения необходимо придерживаться определенных правил:

- Используйте для сайта сложный логин и пароль. Поставьте модули, выводящие CAPTCHA при входе в панель администрирования, ограничьте число попыток ввода пароля. Длина пароля должна составлять не менее 8 символов; обязательно следует использовать и буквы, и цифры.
- Периодически создавайте резервные копии и выполняйте сканирование всех файлов.
- Обеспечьте максимальный уровень защиты для компьютера, с которого осуществляется управление сайтом.
- Используя файловые менеджеры для работы с сайтом, не сохраняйте логин и пароль. Даже если доступ к FTP-серверу открыт только с вашего IP-адреса, остается риск заражения.
- Используйте последнюю версию CMS, своевременно обновляйте ее и все модули.

- Не пользуйтесь взломанными версиями плагинов, компонентов, модулей. Старайтесь приобретать их на хорошо зарекомендовавших себя сайтах разработчиков.

Заключение

Риск посетить инфицированный сайт весьма велик. Опасность заражения состоит в том, что оно часто оказывается незаметным для администратора. При обнаружении симптомов нужно деактивировать сайт, предотвращая дальнейшее распространение вредоносной нагрузки. Для профилактики заражения необходимо придерживаться определенных правил. Обеспечьте максимальный уровень защиты для компьютера, с которого осуществляется управление сайтом.

И так, подведем итоги. Какой антивирус Вы бы ни выбрали, помните следующее: любой антивирус не дает 100% защиты компьютера, так как с каждым часом появляются новые вирусы. Самый лучший антивирус — это голова. Перед каждым открытием файла или страницы сайта, нужно внимательно читать сообщения, не кликать бездумно по баннерам и ссылкам.

Список используемых материалов

Что такое Web-страницы и Web-сайты.

Ссылка- https://webnub.ru/dlya-novichkov/osvoenie-interneta/chto-takoe-web-stranica-sajt/

Заражение веб-сайта

Ссылка- https://www.anti-malware.ru/threats/website-infection

10 лучших бесплатных антивирусов

Ссылка- https://lifehacker.ru/10-luchshix-antivirusov/

Антивирусы. Анализ современных антивирусных программ

Ссылка- https://infourok.ru/individualnyj-proekt-po-discipline-informatika-na-temu-antivirusy-analiz-sovremennyh-antivirusnyh-programm-4374397.html