АНТИВИРУСНЫЕ ПРОГРАММЫ

1 Основы работы антивирусных программ

Общие сведения

Антивирусные программы - это программы, основной задачей которых является защита именно от вирусов, или точнее, от вредоносных программ.

Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

Из всех методов антивирусной защиты можно выделить две основные группы:

Сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов

Эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен

Сигнатурный анализ

Слово сигнатура в данном случае является калькой на английское signature, означающее "подпись" или же в переносном смысле "характерная черта, нечто идентифицирующее". Собственно, этим все сказано. Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами.

Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют антивирусную базу.

Задачу выделения сигнатур, как правило, решают люди - эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. Как правило - потому что в наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур. Например, в случае несложных по структуре троянов или червей, которые не заражают другие программы, а целиком являются вредоносными программами.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вирусов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются. Тем не менее, между антивирусными компаниями существует договоренность об обмене образцами вирусов, а значит рано или поздно сигнатура нового вируса попадает в антивирусные базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех.

Одно из распространенных заблуждений насчет сигнатур заключается в том, каждая сигнатура соответствует ровно одному вирусу или вредоносной программе. И как следствие, антивирусная база с большим количеством сигнатур позволяет обнаруживать больше вирусов. На самом деле это не так. Очень часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому считать, что количество сигнатур равно количеству обнаруживаемых вирусов, уже нельзя.

Соотношение количества сигнатур и количества известных вирусов для каждой антивирусной базы свое и вполне может оказаться, что база с меньшим количеством сигнатур в действительности содержит информацию о большем количестве вирусов. Если же вспомнить, что антивирусные компании обмениваются образцами вирусов, можно с высокой долей уверенности считать, что антивирусные базы наиболее известных антивирусов эквивалентны.

Важное дополнительное свойство сигнатур - точное и гарантированное определение типа вируса. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вируса. Если бы сигнатурный анализ давал только ответ на вопрос, есть вирус или нет, но не давал ответа, что это за вирус, очевидно, лечение было бы не возможно - слишком большим был бы риск совершить не те действия и вместо лечения получить дополнительные потери информации.

Другое важное, но уже отрицательное свойство - для получения сигнатуры необходимо иметь образец вируса. Следовательно, сигнатурный метод непригоден для защиты от новых вирусов, т. к. до тех пор, пока вирус не попал на анализ к экспертам, создать его сигнатуру невозможно. Именно поэтому все наиболее крупные эпидемии вызываются новыми вирусами. С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры почти беспрепятственно. Почти - потому что в защите от новых вирусов помогают дополнительные средства защиты, рассмотренные ранее, а также эвристические методы, используемые в антивирусных программах.

Эвристический анализ

Слово "эвристика" происходит от греческого глагола "находить". Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Поскольку такое определение звучит достаточно сложно и непонятно, проще объяснить на примерах различных эвристических методов

Поиск вирусов, похожих на известные

Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на (весьма правдоподобном) предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных. Постфактум такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов. Основанный на таком предположении эвристический метод заключается в поиске файлов, которые не полностью, но очень близко соответствуют сигнатурам известных вирусов.

Положительным эффектом от использования этого метода является возможность обнаружить новые вирусы еще до того, как для них будут выделены сигнатуры. Отрицательные стороны:

Вероятность ошибочно определить наличие в файле вируса, когда на самом деле файл чист - такие события называются ложными срабатываниями

Невозможность лечения - и в силу возможных ложных срабатываний, и в силу возможного неточного определения типа вируса, попытка лечения может привести к большим потерям информации, чем сам вирус, а это недопустимо

Низкая эффективность - против действительно новаторских вирусов, вызывающих наиболее масштабные эпидемии, этот вид эвристического анализа малопригоден

Поиск вирусов, выполняющих подозрительные действия

Другой метод, основанный на эвристике, исходит из предположения, что вредоносные программы так или иначе стремятся нанести вред компьютеру. Метод основан на выделении основных вредоносных действий, таких как, например:

- Удаление файла.

- Запись в файл.

- Запись в определенные области системного реестра.

- Открытие порта на прослушивание.

- Перехват данных вводимых с клавиатуры.

- Рассылка писем.

- И др.

Понятно, что выполнение каждого такого действия по отдельности не является поводом считать программу вредоносной. Но если программа последовательно выполняет несколько таких действий, например, записывает запуск себя же в ключ автозапуска системного реестра, перехватывает данные вводимые с клавиатуры и с определенной частотой пересылает эти данные на какой-то адрес в Интернет, значит эта программа по меньшей мере подозрительна. Основанный на этом принципе эвристический анализатор должен постоянно следить за действиями, которые выполняют программы.

Преимуществом описанного метода является возможность обнаруживать неизвестные ранее вредоносные программы, даже если они не очень похожи на уже известные. Например, новая вредоносная программа может использовать для проникновения на компьютер новую уязвимость, но после этого начинает выполнять уже привычные вредоносные действия. Такую программу может пропустить эвристический анализатор первого типа, но вполне может обнаружить анализатор второго типа.

Отрицательные черты те же, что и раньше:

- Ложные срабатывания.

- Невозможность лечения.

- Невысокая эффективность.

Дополнительные средства

Практически любой антивирус сегодня использует все известные методы обнаружения вирусов. Но одних средств обнаружения мало для успешной работы антивируса, для того, чтобы чисто антивирусные средства были эффективными, нужны дополнительные модули, выполняющие вспомогательные функции.

Модуль обновления

В первую очередь, каждый антивирус должен содержать модуль обновления. Это связано с тем, что основным методом обнаружения вирусов сегодня является сигнатурный анализ, который полагается на использование антивирусной базы. Для того чтобы сигнатурный анализ эффективно справлялся с самыми последними вирусами, антивирусные эксперты постоянно анализируют образцы новых вирусов и выпускают для них сигнатуры. После этого главной проблемой становится доставка сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу.

Именно эту задачу и решает модуль обновления. После того, как эксперты создают новые сигнатуры, файлы с сигнатурами размещаются на серверах компании - производителя антивируса и становятся доступными для загрузки. Модуль обновления обращается к этим серверам, определяет наличие новых файлов, загружает их на компьютер пользователя и дает команду антивирусным модулям использовать новые файлы сигнатур.

Модули обновления разных антивирусов весьма похожи друг на друга и отличаются типами серверов, с которых они могут загружать файлы обновлений, а точнее, типами протоколов, которые они могут использовать при загрузке - HTTP, FTP, протоколы локальных Windows-сетей. Некоторые антивирусные компании создают специальные протоколы для загрузки своих обновлений антивирусной базы. В таком случае модуль обновления может использовать и этот специальный протокол.

Второе, в чем могут отличаться модули обновления - это настройка действий, на случай, если источник обновлений недоступен. Например, в некоторых модулях обновления можно указать не один адрес сервера с обновлениями, а адреса нескольких серверов, и модуль обновления будет обращаться к ним по очереди, пока не обнаружит работающий сервер. Или же в модуле обновления может быть настройка - повторять попытки обновления с заданным интервалом определенное количество раз или же до тех пор, пока сервер не станет доступным. Эти две настройки могут присутствовать и одновременно.

Модуль планирования

Второй важный вспомогательный модуль - это модуль планирования. Существует ряд действий, которые антивирус должен выполнять регулярно: в частности, проверять весь компьютер на наличие вирусов и обновлять антивирусную базу. Модуль планирования как раз и позволяет настроить периодичность выполнения этих действий.

Для обновления антивирусной базы рекомендуется использовать небольшой интервал - один час или три часа, в зависимости от возможностей канала доступа в Интернет. В настоящее время новые модификации вредоносных программ обнаруживаются постоянно, что вынуждает антивирусные компании выпускать новые файлы сигнатур буквально каждый час. Если пользователь компьютера много времени проводит в Интернете, он подвергает свой компьютер большому риску и поэтому должен обновлять антивирусную базу как можно чаще.

Полную проверку компьютера нужно проводить хотя бы потому, что сначала появляются новые вредоносные программы, а только потом сигнатуры к ним, а значит всегда есть возможность загрузить на компьютер вредоносную программу раньше, чем обновление антивирусных баз. Чтобы обнаружить эти вредоносные программы, компьютер нужно периодически перепроверять. Разумным расписанием для проверки компьютера можно считать раз в неделю.

Исходя из сказанного, основная задача модуля планирования - давать возможность выбрать для каждого действия расписание, которое больше всего подходит именно для этого типа действия. Следовательно модуль обновления должен поддерживать много различных вариантов расписания из которых можно было бы выбирать.

Модуль управления

По мере увеличения количества модулей в антивирусе возникает необходимость в дополнительном модуле для управления и настройки. В простейшем случае - это общий интерфейсный модуль, при помощи которого можно в удобной форме получить доступ к наиболее важным функциям:

- Настройке параметров антивирусных модулей.

- Настройке обновлений.

- Настройке периодического запуска обновления и проверки.

- Запуску модулей вручную, по требованию пользователя.

- Отчетам о проверке.

- Другим функциям, в зависимости от конкретного антивируса.

Основные требования к такому модулю - удобный доступ к настройкам, интуитивная понятность, подробная справочная система, описывающая каждую настройку, возможность защитить настройки от изменений, если за компьютером работает несколько человек. Подобным модулем управления обладают все антивирусы для домашнего использования. Антивирусы для защиты компьютеров в крупных сетях должны обладать несколько иными свойствами.

Уже не раз говорилось, что в большой организации за настройку и правильное функционирование антивирусов отвечают не пользователи компьютеров, а специальные сотрудники. Если компьютеров в организации много, то каждому ответственному за безопасность сотруднику придется постоянно бегать от одного компьютера к другому, проверяя правильность настройки и просматривая историю обнаруженных заражений. Это очень неэффективный подход к обслуживанию системы безопасности.

Поэтому, чтобы упростить работу администраторов антивирусной безопасности, антивирусы, которые используются для защиты больших сетей, оборудованы специальным модулем управления. Основные свойства этого модуля управления:

· Поддержка удаленного управления и настройки - администратор безопасности может запускать и останавливать антивирусные модули, а также менять их настройки по сети, не вставая со своего места.

· Защита настроек от изменений - модуль управления не позволяет локальному пользователю изменять настройки или останавливать антивирус, чтобы пользователь не мог ослабить антивирусную защиту организации.

Это далеко не все требования к управлению антивирусной защитой в крупной организации, а только основные принципы. Подробнее об особенностях антивирусной защиты сетей и требованиях к модулям управления будет рассказано позже в соответствующем разделе.

Карантин

Среди прочих вспомогательных средств во многих антивирусах есть специальные технологии, которые защищают от возможной потери данных в результате действий антивируса.

Например, легко представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивируса. Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит с определенной вероятностью антивирус мог удалить незараженный файл.

Или же антивирус обнаруживает важный документ зараженный вирусом и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченным вирусом теряется важная информация.

Разумеется, от таких случаев желательно застраховаться. Проще всего это сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда если окажется, что файл был удален ошибочно или была потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

Тестирование работы антивируса

После того как антивирус установлен и настроен, каждый пользователь хочет убедиться, что он все сделал правильно и антивирусная защита работает. Но как это проверить? Первое, что приходит в голову: взять где-нибудь зараженный файл и посмотреть поймает ли его антивирус. Но, как и у многих простых решений, у этого есть ряд очевидных недостатков:

· Зараженный файл не так-то просто найти. Даже если воспользоваться поиском в Интернете и найти какие-то файлы, нет никакой гарантии, что они действительно заражены. Т. е. если антивирус обнаружит в них вирусы, значит они заражены, а антивирус работает, но если не обнаружит, то неизвестно - антивирус не работает, или файлы не заражены

· Использовать для тестирования настоящие вирусы крайне опасно. Если пользователь все же ошибся и неправильно выполнил установку или настройку антивируса, в процессе тестирования он может на самом деле заразить свой компьютер, в результате чего потерять данные или стать источником заражения для других компьютеров.

Значит нужен такой способ тестирования антивирусов, который был бы безопасным, но давал четкий ответ на вопрос, корректно ли работает антивирус. Понимая важность проблемы, организация EICAR при участии антивирусных компаний создала специальный тестовый файл, который был назван по имени организации - eicar.com.

Eicar.com - это исполняемый файл в COM-формате, который не выполняет никаких вредоносных действий, а просто выводит на экран строку "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!". Тем не менее, все антивирусные компании договорились включить этот файл в свои антивирусные базы и детектировать его как вирус, специально чтобы пользователи могли без риска протестировать свою антивирусную защиту.

Получить eicar.com можно на сайте организации EICAR по адресу http://www.eicar.org/anti\_virus\_test\_file.htm, но проще создать этот файл самому. Дело в том, что машинный код файла eicar.com состоит из печатных символов и его можно создать при помощи любого текстового редактора. Например, можно воспользоваться стандартным для операционных систем Windows редактором Notepad. В окне Notepad нужно набрать

сохранить файл под именем eicar.com, и все - тестовый файл готов.

Рис. 1 - Тестовый файл eicar.com

Созданный описанным способом файл eicar.com ничем не отличается от доступного на сайте организации EICAR, можно загрузить и убедиться самому. Его можно пытаться скопировать на защищенную машину, запускать на ней или же просто проверять, чтобы проверить работу антивируса в разных режимах.

Тестирование антивируса при помощи eicar.com тоже не идеально. Концепция тестового файла и сам тестовый файл, разрабатывались в начале 90-х годов, когда едва ли не единственным типом вредоносных программ были файловые вирусы. Поэтому eicar.com в первую очередь позволяет протестировать, как антивирус справляется с файловыми вирусами и близкими по структуре вредоносными программами - большинством троянов, некоторыми червями.

Однако сейчас разнообразие вредоносных программ гораздо больше. И соответственно больше антивирусных модулей, предназначенных для защиты от различных угроз. Например, во многих антивирусах имеется специальный модуль защиты от скрипт-вирусов, а поскольку eicar.com скрипт-вирусом не является, он непригоден для тестирования таких модулей. Точно так же eicar.com непригоден для тестирования специальных модулей для защиты от макровирусов. К сожалению, на сегодняшний день новых способов тестирования антивирусных средств, которые поддерживались бы всеми производителями антивирусов нет, и приходится полагаться на старые способы.

2 Классификация антивирусов

Общие сведения

Обязательное свойство любой качественной защиты - это способность не мешать выполнению основных функций защищаемой системы, предмета или человека. Такая защита должна обеспечивать безопасность, не вмешиваясь в деятельность защищаемого объекта, по возможности быть невидимой, ее влияние - сведено к минимуму. Однако от этого ни в коем случае не должна страдать надежность.

В случае антивирусной защиты такой баланс обычно достигается путем введения двух различных режимов работы антивирусных программ с возможностью самостоятельной подробной настройки пользователем параметров каждого из них, а также разработки отдельных программных комплексов для компьютеров, выполняющих разные функции.

Режимы работы антивирусов

Надежность антивирусной защиты обеспечивается не только способностью отражать любые вирусные атаки. Другое не менее важное свойство защиты - ее непрерывность. Это означает, что антивирус должен начинать работу по возможности до того, как вирусы смогут заразить только что включенный компьютер и выключаться только после завершения работы всех программ. Однако с другой стороны, пользователь должен иметь возможность в любой момент запросить максимум ресурсов компьютера для решения своей, прикладной задачи и антивирусная защита не должна ему помешать это сделать. Оптимальный выход в этой ситуации - это введение двух различных режимов работы антивирусных средств: один с небольшой функциональностью, но работающий постоянно, и второй - тщательная и более ресурсоемкая проверка на наличие вирусов по запросу пользователя. Такое разделение принято в большинстве современных антивирусов.

Проверка в режиме реального времени

Проверка в режиме реального времени, или постоянная проверка, обеспечивает непрерывность работы антивирусной защиты. Это реализуется с помощью обязательной проверки всех действий, совершаемых другими программами и самим пользователем, на предмет вредоносности, вне зависимости от их исходного расположения - будь это свой жесткий диск, внешние носители информации, другие сетевые ресурсы или собственная оперативная память. Также проверке подвергаются все косвенные действия через третьи программы.

Требование к невмешательству осуществляется с помощью задания персональных настроек, наиболее точно отражающих специфику конкретного компьютера. В большинстве случаев, например, можно безболезненно отключить из проверки файлы ряда графических форматов, текстовые файлы, архивы (поскольку при распаковке все содержащиеся в архиве файлы все равно будут проверены), исходящую почту.

Постоянная проверка защиты системы от заражения необходима даже в случае, если вредоносный код каким-либо способом уже проник на компьютер - например, еще до установки антивируса. Следовательно, этот режим должен быть включен с момента начала загрузки операционной системы и выключаться только в последнюю очередь.

Проверка по требованию

В некоторых случаях наличия постоянно работающей проверки в режиме реального времени может быть недостаточно. Возможна ситуация, когда на компьютер был скопирован зараженный файл, исключенный из постоянной проверки ввиду больших размеров и, следовательно, вирус в нем обнаружен не был. Если этот файл на рассматриваемом компьютере запускаться не будет, то вирус может остаться незамеченным и проявить себя только после пересылки его на другой компьютер, что может сильно повредить репутации отправителя - распространителя вирусов. Для исключения подобных случаев используется второй режим работы антивируса - проверка по требованию.

Для такого режима обычно предполагается, что пользователь лично укажет какие файлы, каталоги или области диска необходимо проверить и время, когда нужно произвести такую проверку - в виде расписания или разового запуска вручную. Обычно рекомендуется проверять все чужие внешние носители информации, такие как дискеты, компакт диски, flash-накопители каждый раз перед чтением информации с них, а также весь свой жесткий диск не реже одного раза в неделю.