Анализ АНТИВИРУСНЫХ средств

Мария Кузнецова, *менеджер по маркетингу LETA IT-company*

Компьютерные вирусы и борьба с ними сегодня являются наиболее популярными темами при обсуждении вопросов, связанных с безопасностью информации. Просматривая статьи и вырезки, посвященные атакам на компьютерные системы, нередко обнаруживаешь в них упоминание о компьютерных вирусах, а так же об атаках на отказ в обслуживании, с помощью этих вирусов проводимые.

Борьба с вирусами не прекращается ни на минуту. Методики становятся все более изощренными, системы защиты многоуровневыми и многокомпонентными, а время реакции на события все меньше. Но, несмотря на все усилия разработчиков антивирусного программного обеспечения, тенденция остается неизменной: эпидемии становятся все масштабнее, а ущерб от них все значительнее.

Чтобы обезопасить себя от неминуемых рисков, связанных с распространением вредоносного кода, следует четко понимать, что не любой антивирус может подойти именно вам.

Как работает антивирус?

Сейчас антивирусное ПО действуют, как правило, по двум алгоритмам: во-первых, выискивается так называемая «сигнатура», во-вторых, применяется так называемая «эвристическая» техника.

Сигнатуры

Антивирус может обнаружить вредоносную программу, будь то резидентный вирус, почтовый червь, троян, backdoor и т. д. — по определенной последовательности байтов, которая и называется «сигнатурой». Метод сигнатур заключается в следующем: в базе антивируса имеются сигнатуры (определённые признаки), по которым можно опознать какой-либо вирус. Сигнатура – это уникальная байтовая последовательность, наличие которой является признаком данного файла, и на основании которой проводится соотнесение файла к соответствующей категории – «заражен», «не заражен». Вирус, как и любая другая программа, имеет определенное алгоритмическое решение, которое в зараженном файле будет выглядеть в виде уникальной последовательности байт по определенному смещению. Таким образом, признак зараженности файла вирусом при сигнатурном анализе можно представить в виде:

ЕСЛИ ((Файл Содержит (Файл1, Последовательность Вируса) = Правда) И (Смещение В Файле (Файл1, Последовательность Вируса) = Смещение Вируса)) ТО Файл1 – заражен.

Как можно догадаться, у сигнатурного метода низкий уровень интеллектуальности. Т. е., если появился новый вирус, сигнатура которого не имеется в базе антивируса, то пользователь от него не защищён. Дело в том, что в антивирусных базах хранятся десятки тысяч таких сигнатур, однако против совершенно нового вируса, сигнатура которого в базе отсутствует, антивирусный пакет оказывается бессилен. В прежние времена, когда вирусы распространялись в основном на носителях информации, вроде дискет, – то есть, довольно медленно, – поставщики антивирусных решений успевали создать противоядие до того, как вирус получал широкое распространение. Кроме этого, сигнатурный метод бесполезен против самомодифицирующихся вирусов, ведь раз изменён вирус, то и его сигнатура изменилась.

Эвристика

Эвристический же метод предусматривает проверку всех команд программы и выявление «подозрительных» действий. Эвристические технологии могут выявлять новые вирусы, никогда ранее не встречавшиеся, и, таким образом, способны предотвращать распространение опасного программного кода. Однако эвристические методы нередко дают ложные предупреждения, принимающие обычную программу за вирус.

В последнее время антивирусные компании стали совмещать эти методы в работе своих продуктов, т. к. в комбинации эти методы более эффективны, чем по отдельности.

Современные антивирусы, использующие оба метода, часто производят эмуляцию процессора, или изолируют полученные из Интернета исполняемые файлы на время выполнения загружаемого кода во внешнюю оболочку, где программа неспособна нанести вред системе.

Антивирусная система, работающая по методу «блокировки по поведению» позволяет антивирусу в реальном времени отслеживать действия работающих программ и блокировать те действия, которые могут напоминать работу антивируса. К таким действиям относятся, в частности, несанкционированные попытки открыть, просмотреть, удалить или изменить файлы, отформатировать диск или произвести с ним какие-то другие операции с необратимыми последствиями. Это могут быть изменения в логике работы программ, скриптов или макросов, модификация в ключевых установках системы; несанкционированные попытки переслать по почте или через интернет-пейджеры исполняемых файлов. Или также несанкционированные попытки установить сетевые соединения. Кроме того, как бы ни маскировался вирус, рано или поздно он выдает себя вполне конкретным запросом к операционной системе, так что у антивируса всегда есть возможность его обнаружить и истребить.

Однако при использовании этого метода подозрительные программы подвергаются лишь частичному сканированию, и весь набор их команд может и не быть проверен. Из-за того, что существует огромное

количество способов закамуфлировать вредоносную программу, даже при совместном использовании этих методов они не всегда могут обнаружить новую заразу. Кроме того, чтобы антивирус мог вычислить все повадки вируса, тот должен запуститься в системе. А соответственно – нанести вред.

Сейчас очень возросла конкуренция между производителями антивирусных программ. Из-за этого в сигнатурных базах имеются все известные вирусы. А вот основной упор идёт на эвристический метод обнаружения, т. к. участились не массовые вирусные атаки, а точечные. Большинство вирусов создаётся для определённых лиц/фирм/контор и за пределы цели вирус не выходит. Следовательно, вероятность попадания вируса в руки антивирусной компании — для его изучения и выпуска обновления — очень мала. Тем более, что в Интернете появилось множество документаций по написанию/модифицированию вирусов. Получается, что лучший антивирус тот, который сможет обнаружить неизвестные вирусы. Так же производители антивирусных средств, для большей популярности, встраивают в свои продукты различные дополнительные модули.

Каждый пользователь или администратор, создающий антивирусную защиту, обязательно столкнется с проблемой выбора наиболее подходящей антивирусной программы. Однако выбор антивируса – далеко не такая простая задача, как это может показаться на первый взгляд. Доверившись советам знакомых, можно получить совсем не тот результат, которого хотелось бы.

При сравнении антивирусов в первую очередь следует учитывать их способность решать свою главную задачу, а именно находить и уничтожать вирусы. Такую информацию можно почерпнуть из независимых подробных сравнений и тестов антивирусного ПО, проводимых авторитетными экспертами. Среди них хочу выделить West coast labs, Checkmark, AV-Comparatives. org Andreas Clementi и PCMag, издающийся в Великобритании Virus Bulletin, объединивший в себе экспертов в области антивирусной защиты с мировыми именами: Network Associates, Sophos Plc, Symantec Corporation, IBM Research, WildList Organization International, Aladdin Knowledge Systems Ltd. В январе 1998 года журнал Virus Bulletin учредил награду VB100 %, которой отмечаются антивирусы, способные наилучшим образом обнаруживать «живые» вирусы, встречающиеся в реальной жизни. При этом учитываются самые новые, только что созданные вирусы, собранные организацией WildList Organization International по всему миру, а не из одного или нескольких мест. Именно такие вирусы представляют собой наибольшую угрозу.

Ниже приведена сравнительная таблица основных характеристик наиболее сильных игроков рынка антивирусной защиты (на основе данных VB, West coast labs, Checkmark, AV-Comparatives. org Andreas Clementi и PCMag.):

	ESET NOD32	Kaspersky	BitDefender	Trend Micro	Symantec	McAfee
Минимальная цена (Std, для рабочих станций, один пользователь)	$39,00	$39,00	$29,74	$43,01	$32,00	$67,00
Продуктовая линейка	Bad	Avarage	Good	Very good	Very good	Good
Особенности						
Количество наград VB100%	38	33	12	14	33	26
ICSA 2005 Certified	+	+	+	+	+	+
W.C.L Level 1 Certified	+	+	+	+	+	+
W.C.L Level 2 Certified	+	+	+	+	+	+
Среднее время обновления АВ баз	Ежедневно	раз в 1 час	раз в 2-3 часа	Ежедневно	Еженедельно	Ежедневно
Средняя скорость сканирования	7,49 МБ/сек	3,55 МБ/сек	3,93 МБ/сек	n/a	5,64 МБ/сек	5,50 Мб/сек
Возможности сканирования						
Возможность резидентного сканирования	+	+	+	+	+	+
Возможность сканирования в режиме реального времени	+	+	+	+	+	+
Возможность сканирования по требованию	+	+	+	+	+	+
Возможность сканирования по расписанию	+	+	+	+	+	+
Эвристический механизм сканирования	High	Low	High	None	None	Low
Возможность ручного сканирования	+	+	+	+	+	+
Возможность сканирования Adware/spyware	+	+	+	+	+	+
Наличие технологий скрипт-блокирования	+	+	+	+	+	+
Возможность сканирования архивов	+	+	+	+	+	+
Возможность автоматического лечения зараженного объекта	+	+	+	+	+	+
Возможность карантина зараженного объекта	+	+	+	+	+	+
Наличие защиты электронной почты (POP3)	+	+	+	+	+	+
Возможность защиты реестра при загрузке системы	-	-	+	-	-	-

Возможность сканирования документов MS Office	+	+	+	+	+	+
Обновления						
Цена продления лицензии	скидка 40%	скидка 30%				
Возможность автоматического обновления баз	+	+	+	+	+	+
Возможность автоматического обновления программных компонентов	+	+	+	+	-	+
Возможность ручного обновления баз	+	+	+	+	+	+
Возможность ручного обновления программных компонентов	+	+	+	+	-	+
Возможность создания локальной папки обновлений в сети	+	+	+	+	-	-
Другие особенности						
Антивирусный сканнер в режиме Online	-	+	+	+	-	+
Возможность защиты паролем настроек программы	+	+	+	+	+	+
Способность обнаружать абсолютно новые вирусы (Zero day Protect)	+	+	-	-	-	-
Возможность централизованной установки и администрирования	+	+	+	+	+	+
Техническая поддержка						
Общение в режиме Online	icq (русский)	-	icq (русский)	-	-	chat (англ.)
Поддержка по телефону НА РУССКОМ ЯЗЫКЕ	+	+	+	+	-	-
Документация/FAQ/База знаний	+	+	(англ.)	(англ.)	(англ.)	(англ.)
Форум пользователей	+	+	-	-	-	-
Поддержка по электронной почте	+	-	+	-	-	+
Поддержка через Веб-форму	+	+	+	+	+	-
Наличие встроенной контекстной русскоязычной справки	+	+	-	+	+	-
Поддерживаемые конфигурации						
Windows 2003	+	+	+	+	+	+
Windows XP	+	+	+	+	+	+
Windows 2000	+	+	+	+	+	+
Windows ME	+	+	+	+	+	+
Windows NT	+	+	+	+	+	+
Windows 98	+	-	+	+	+	+
Windows 95	+	-	-	+	-	-
Linux/UNIX	+	+	+	+	-	+
Lotus Domino	+	+	+	+	+	+
Novell NetWare	+	+	-	+	+	+
Поддержка x64 битных платформ	+	-	-	+	-	-
Виды защиты						
Аппаратная защита по периметру	-	-	-	+	+	-
Защита шлюзов	-	+	+	+	+	+
Защита рабочих станций	+	+	+	+	+	+
Защита почтовых серверов	+	+	+	+	+	+
Защита файловых серверов	+	+	+	+	+	+
Защита информационных порталов	-	-	+	+	+	+
Защита серверов - хранилищ	+	-	-	-	+	-
Защита мобильных устройств	-	+	-	+	+	+

В заключение хочется добавить, что при выборе антивируса, помимо экспертных оценок авторитетных специалистов, нелишне знать простые истины:

- Цена, известность, рекламный шум не обязательно отражает качество.
- «Защищает от всех известных вирусов!» — это рекламный трюк. Любой антивирус защищает от всех известных только ему вирусов, даже если их всего 2.
- Не все файлы, зараженные известным вирусом, могут быть вылечены.
- То, что не лечит один антивирус — может лечить другой.
- Скорость проверки не говорит о качестве, «тщательности» проверки.