РАЗРАБОТКА МЕТОДИКИ СРАВНИТЕЛЬНОГО ТЕСТИРОВАНИЯ АНТИВИРУСНЫХ ПРОДУКТОВ

А.А. Калашникова, Д.А. Калинин, А.В. Клейменов, В.Д. Стремоухов, А.А. Янковская
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В настоящее время существует большое количество методик сравнения антивирусных продуктов, но, по мнению автора, они не в полной степени соответствуют всем необходимым критериям. Поэтому целью исследования является разработка открытой и универсальной методологии, позволяющей получить максимально объективные и достоверные результаты.

Введение

В настоящее время нет недостатка в информации о тестировании антивирусов (www.anti-malware.ru, www.antivirus.ru/AntiVirPS.html, www.virusbtn.com, www.av-comparatives.org и пр.). Причем, сколько тестирований, столько и выводов. Практически любой антивирус может стать по итогам тестирования самым лучшим. Результаты тестирований и присваиваемые рейтинги по этим результатам зачастую имеют противоположные оценки. Причина этих расхождений – не в неточности или обмане пользователей, а в различных условиях проведения и критериях выбора лучшего антивируса.

Целью данного исследования является разработка методики сравнительного тестирования антивирусных продуктов, которая имела бы следующие качества:

- адекватность;
- открытость, т.е. чтобы тестирование по ней можно было бы повторить кому угодно с получением таких же результатов;
- универсальность, т.е. должна охватывать наиболее важные критерии, в соответствии со спецификой тестируемых продуктов;
- носить технический характер, т.е. отвечать на вопрос, насколько хорошо тот или иной продукт будет защищать компьютер от вредоносного кода, не затрагивая вопросы юзабилити, дополнительных функций и т.п.

Основными задачами данного исследования являются исследование существующих методик, формирование списка критериев, выбор продуктов тестирования, проведение эксперимента.

Существующие методологии

Характер компьютерных угроз постоянно меняется, и по мере того, как они становятся все более изощренными, уже ни одна технология не может гарантировать 100% защиты. Хотя пользователи сами вынуждены решать, какие средства применять, задачу выбора им существенно упрощают независимые тестирования продуктов, проводимые специализированными агентствами.

Установка антивирусного программного обеспечения сегодня обязательна для всех пользователей ПК, обеспокоенных проблемой безопасности данных. Выбирая тот или иной продукт, они стремятся сделать защиту максимально надежной. А подробную информацию о рассматриваемых антивирусных средствах могут получить из отчетов по результатам тестирований [1].

Исследование надежности антивирусов в основном сводится к проверке эффективности ПО в реальных условиях. Однако подходы к проведению тестирования могут различаться. В антивирусной индустрии существует и вполне научный, признанный всеми основными игроками подход к тестированию антивирусного ПО. Базируется он на деятельности некоммерческой организации WildList (www.wildlist.org), которая сама тестированиями не занимается, а предоставляет тестерам вирусные базы.

«Дикие» вирусы. WildList (www.wildlist.org) – международная организация, созданная для сбора и обобщения информации о вирусах, атакующих компьютеры пользователей по всему миру. Основное понятие, используемое в проекте WildList – это термин «дикий вирус» («In the Wild», или сокращенно ITW).

«Дикие вирусы» – это вирусы, свободно распространяющиеся по Всемирной сети и периодически атакующие компьютеры пользователей. Списки «диких вирусов» составляются каждый месяц и предоставляются для тестирований антивирусов независимым исследовательским агентствам.

Список «диких вирусов» включает только те вирусы, которые, во-первых, обнаружены более чем двумя респондентами более чем в двух различных местах (сообщившие о вирусе специалисты должны принадлежать к разным компаниям и обнаружить вирус различными способами, т.е. обнаружение одним антивирусом не считается явным доказательством его «дикости»), во-вторых, являются реальными malware, самораспространяющимися и несущими вред либо представляющими угрозу информационной безопасности пользователей.

Сама организация WildList лишь собирает и анализирует информацию о вредоносных программах. Тестированием антивирусного ПО, отталкиваясь от списка «In The Wild», занимаются такие компании, как ICSA Labs, West Coast Labs и Virus Bulletin. Надо заметить, что абсолютно все известные производители антивирусного ПО тестируют свои продукты в этих исследовательских компаниях. Сегодня такие испытания стали единственным общепризнанным инструментом, позволяющим сделать объективный вывод об эффективности того или иного антивируса. Формат предоставления данных исследователями обычно позволяет хронологически проследить надежность каждого продукта от версии к версии и от платформы к платформе [2].

Сертификация ICSA. ICSA (www.icsalabs.com) – International Computer Security Association (Международная компьютерная ассоциация по защите) – начала свою деятельность в 1992 г. В тестированиях, проводимых ICSA Labs, используется вредоносный код как из собственной «коллекции», так и из списка «In The Wild». По результатам исследований продуктам выдается сертификат ICSA – его удостаиваются те антивирусы, которые способны обнаружить 100% вирусов из списка «In The Wild», выпущенного за месяц до испытаний, и не менее 90% из вирусов собственной коллекции ICSA. Дополнительно антивирусы проверяются на наличие ложных срабатываний. Сертификацию ICSA способно пройти большинство существующих на рынке антивирусов. Данный сертификат есть практически у всех более-менее известных продуктов.

West Coast Labs/ Checkmark. West Coast Labs (www.check-mark.com**)** – один из мировых лидеров в области тестирования ПО для защиты от угроз. По результатам испытаний в West Coast Labs антивирусным продуктам выдается сертификат CheckMark.

В рамках сертификации CheckMark продукты тестируются по категориям. Сегодня это 4 типа испытаний и, соответственно, 4 типа сертификатов:

- Anti-Virus Level 1. Испытываемый продукт должен распознать все вирусы из списка «In The Wild», выпущенного за два месяца до даты тестирования.
- Anti-Virus Level 2. Антивирус, получивший этот сертификат, должен не только обнаружить, но и вылечить систему от всех вирусов, найденных в Level 1.
- Trojan. Проверяется возможность антивируса бороться с вредоносным кодом категории «трояны». Тестирование проводится на базе образцов, отобранных специалистами West Coast Labs.
- Spyware. Антивирусы тестируются на способность противостоять «шпионским программам» (spyware). Тестирование проводится на базе образцов, отобранных специалистами West Coast Labs.

Сертификатами Anti-Virus Level 1 и Anti-Virus Level 2 обладает очень большое количество антивирусов. Прежде всего, это говорит о том, что большинству антивиру-

сов не составляет труда обнаружить и обезвредить вирусы из списка «In The Wild», выпущенного за 2 месяца до даты тестирования. Список антивирусного ПО, имеющего сертификат CheckMark категории «Trojan», существенно короче – пройти это тестирование оказывается для многих компаний уже сложнее. А сертификатами CheckMark в категории «Spyware» обладает совсем небольшое количество продуктов.

Британский «бюллетень». Virus Bulletin (www.virusbulletin.com) – наиболее известный и авторитетный в мире британский журнал, посвященный антивирусам. Тестирования, которые проводятся журналом Virus Bulletin, также основываются на списке вирусов «ln The Wild». Успешно прошедшие испытания продукты получают награду «VB100%». Тестирования проводятся регулярно, несколько раз в год для разных платформ.

Особенность Virus Bulletin – в том, что в испытаниях используется список, выпущенный лишь за две недели до даты испытаний. Параллельно при этом антивирус тестируется на заведомо чистых от вирусов файлах – на наличие ложных срабатываний. Компании, предоставившие свой продукт для тестирования, никогда заведомо не знают, пройдет ли их антивирус испытания успешно. В отличие от других исследователей, Virus Bulletin обязательно информирует своих читателей не только об успехах, но также и о неудачах антивирусных программ. В последнем случае они получают специальный значок, свидетельствующий о том, что антивирус тест не прошел.

Важная особенность методики Virus Bulletin состоит в том, что награда VB100% присуждается продукту не обязательно в случае обнаружения им 100% угроз: допускается возможность пропустить некоторый процент вредоносных программ. Например, если антивирус нашел 98%, то награду он все равно получит. Сегодня многие производители антивирусного ПО заявляют, что смогут гарантированно обнаружить угрозу через один или два часа после ее появления. Но, как показывают тестирования Virus Bulletin, огромное количество вирусов пропускается и через 2 недели после их обнаружения.

В последнее время антивирусная индустрия сталкивается с необходимостью противостоять не только уже обнаруженным вирусам, но также и еще не известным угрозам. Чтобы оценить надежность защиты от еще не существующих угроз, требуются особые методики тестирования. Традиционные испытания здесь бессильны, так как в них исследуется способность антивируса противостоять угрозам, которые уже обнаружены и включены в вирусную базу.

С одной стороны, можно просто попробовать отключить у тестируемого антивирусного продукта сигнатурные базы и посмотреть, как он без них сможет обнаружить вирусы из актуального списка «In The Wild». Но этот путь не приведет к получению полезного и значимого результата: сама технология работы антивирусных программ не предполагает отключения сигнатурных баз. Антивирус с отключенными сигнатурными базами – уже совсем другой продукт, тестировать который не имеет смысла.

С другой стороны, способность антивируса противостоять еще не существующим угрозам можно проверить, используя в тестировании актуальную вирусную базу, но испытывая антивирус с сигнатурной базой, скажем, полугодовой давности. Ведь те вирусы, которые есть в актуальном списке ITW, полгода назад еще не существовали. Продукту, таким образом, придется противостоять несуществующим угрозам. Ресурс Андреаса Клименти www.av-comparatives.org специализируется именно на таких тестированиях. На сайте можно познакомиться с результатами ретроспективных тестов, которые могут оказаться не только полезны при выборе антивируса, но и просто любопытны.

На сайте Virus Bulletin говорится: «Если какой-либо антивирус не прошел наш тест, то это еще не значит, что он неэффективен. Он неэффективен только в руках неподготовленного пользователя. Специалист же сможет его использовать совершенно

по-иному». Один из выводов, который можно сделать после изучения разных методик тестирования и результатов испытаний, состоит в том, что, к сожалению, сегодня ни один продукт не способен гарантировать 100%-защиту от связанных с вредоносным кодом угроз. Однако полное представление о существующей опасности и правильный выбор методов защиты способны свести возможность заражения к минимуму [3].

Разрабатываемая методика

Были выбраны следующие критерии:

- уровень детектирования вирусной коллекции,
- уровень детектирования «in the wild»,
- процент ложных срабатываний,
- эвристический анализ,
- эмуляция,
- лечение активного заражения.

Из них наиболее критичными являются:

- уровень детектирования «коллекции»,
- уровень детектирования «In The Wild»,
- процент ложных срабатываний,
- эвристический анализ.

1) Уровень детектирования вирусной коллекции. В каждом тестируемом антивирусе запускается сканирование по требованию каталога с огромным количеством вирусных экземпляров («коллекция»). Уровень детектирования определяется процентным соотношением количества вредоносных объектов к общему числу проверенных файлов.

2) Уровень детектирования «In The Wild». Данный критерий подразумевает проверку образцов взятых из списка in the wild. Данный параметр определяется отношением обнаруженных вредоносных объектов к общему количеству объектов.

3) Процент ложных срабатываний (false-alarms). Проверяется на коллекции с большим количеством файлов, не относящихся к вредоносным, затем считается количество ложных срабатываний и высчитывается отношение количества ложных срабатываний к общему количеству файлов.

4) Эвристический анализ. Это метод работы антивирусной программы, основанный на сигнатурах и эвристике, он призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда сигнатура совпадает с телом неизвестной программы не на 100 %, но в подозрительной программе налицо более общие признаки вируса. Данная технология, однако, применяется в современных программах очень осторожно, так как может повысить количество ложных срабатываний [4].

У всех антивирусов необходимо отключить функцию обновления, т.е. заморозить антивирусные базы данных на дату начала теста.

Сканирование ITW-образцов. Сканирование по требованию производится с максимально возможными настройками: включение эвристики (максимальный уровень), проверка всех файлов, обнаружение всех типов вредоносных и потенциально опасных программ.

5) Эмулятор. Эвристические методы нацелены на исследование файла, который не опознается сигнатурным сканером в качестве подозрительного или вредоносного. Их задача состоит в обнаружении еще не известных антивирусной компании вредоносных программ. Эвристических технологий достаточно много, среди них можно выделить основные.

- Сигнатурный метод. Основан на поиске характерных для вредоносной программы фрагментов кода и (или) констант.

- Эмулятор. Как следует из названия, его задачей является эмуляция выполнения изучаемой программы. Качество эмуляции может быть разным – от примитивной эмуляции команд без эмуляции API функций до почти идеальной эмуляции работы программы в операционной системе. Хороший эмулятор является очень мощным инструментом для выявления новых видов malware, однако он уязвим перед специальными методиками защиты – так называемыми антиэмуляторами.
- Эмулятор и сигнатурный анализ. Также возможно использование одновременно двух вышеперечисленных эвристических технологий для детектирования еще не известных видов вредоносных программ, когда возможности эмулятора дополняются поиском в объекте специфических фрагментов кода [5].

Для сравнительного тестирования необходимо отбирать только те антивирусные программы, которые содержат в себе хоть какой-то эмулятор. Специально для данного антивирусного сравнения должны быть подготовлены тестовые образцы (мини-программы), моделирующие поведение вредоносных программ. К каждому образцу следует подготовить краткое описание. В тестовых образцах используются только тривиальные методы, доступные каждому начинающему программисту.

6) Лечение активного заражения. Данное тестирование заключается в изучении способностей антивирусных программ в лечении активного заражения, когда вредоносная программа уже была ранее запущена и установлена на компьютере и более того, может препятствовать детектированию и удалению со стороны различных антивирусных продуктов. Если вредоносный код не детектируется автоматически антивирусным монитором, то инициируется проверка по требованию каталога (или нескольких каталогов), где должны были быть расположены файлы вредоносной программы. Для каждого отобранного семпла вредоносной программы выделялась своя чистая виртуальная машина. После попытки установки какого-либо антивируса и лечения заражения, машина откатывалась в первоначальное состояние.

Для проведения тестирования антивирусов на лечение активного заражения экспертной группой Anti-Malware.ru отбирались вредоносные программы по следующим критериям:

1. детектирование родительского файла всеми участвующими в тесте антивирусами;
2. способность маскировать свое присутствие;
3. способность противодействовать обнаружению со стороны антивируса;
4. способность восстанавливаться в случае удаления некоторых компонент;
5. распространенность и известность.

В отборе вредоносных программ для теста отдавался приоритет наиболее сложным семплам, которые больше удовлетворяют приведенным выше критериям. Стоит отметить, что критически важным параметром для отбора вредоносных программ для теста было детектирование их со стороны всех участвовавших в тесте антивирусов. Все используемые в тесте вредоносные программы были собраные экспертами Anti-Malware.ru во время распространения в Интернет (In The Wild). Каждый отобранный экземпляр вредоносной программы проверялся на работоспособность и установку на тестовой системе [6].

Методология теста антивирусов на статическое сканирование

Тест проводился на специально подготовленном стенде под управлением VMware Workstation 6.0. Для каждого антивирусного продукта клонировалась «чистая» виртуальная машина с операционной системой Microsoft Windows XP SP2. В тестировании участвовали следующие антивирусные программы:

1. Avira Antivir Personal Edition Premium 7.0,
2. DrWeb 4.44,

3. Eset Nod32 Antivirus 3.0,
4. Kaspersky Anti-Virus 7.0,
5. McAfee VirusScan Enterprise 8.5,
6. Norton Anti-Virus 15.5,
7. Trend Micro Antivirus 16.0.

При установке антивирусов производились все рекомендуемые программой действия (перезагрузка системы, обновление и т.д.). Настройки антивирусов не изменялись и оставались установленными по умолчанию.

Шаги проведения тестирования:

1. включение виртуальной машины;
2. проверка коллекции отобранных вредоносных программ сканером по требованию;
3. подсчет детектируемых файлов.

Для каждой антивирусной программы выделялась отдельная чистая виртуальная машина. Сканировалась коллекция записанная на внешнем жестком диске.

В каждом тестируемом антивирусе запускалась задача сканирования по требованию каталога с огромным количеством вирусных экземпляров. Тестовая база вирусов насчитывала 64446. Коллекция сформирована путем поиска в Интернете и системы honeypot. Вирусы в коллекции не повторяются. Все вирусные экземпляры были распакованы (не было файлов zip, rar, ace и т.д.). Также все тестируемые программы на момент тестирования имели актуальные версии с обновленными базами данных.

Результаты сравнительного тестирования

Отобранные 7 антивирусов показали следующие результаты по обнаружению вредоносных программ:

1. Avira Antivir Personal Edition Premium 7.0 – 61,82%;
2. DrWeb 4.44 – 69,17%;
3. Eset Nod32 Antivirus 3.0 – 60,57%;
4. Kaspersky Anti-Virus 7.0 – 61,38%;
5. McAfee VirusScan Enterprise 8.5 – 96,07%;
6. Norton Anti-Virus 15.5 – 43,84%;
7. Trend Micro Antivirus 16.0 – 87,34%.

Наименование	Всего	Вирусов	%	Позиция в рейтинге
McAFee	65169	62605	96,07	1
TrendMicro	64450	56291	87,34	2
DrWeb	86190	59621	69,17	3
Avira	76919	47552	61,82	4
Kaspersky	109490	67205	61,38	5
Eset	84295	51059	60,57	6
Symantec	84427	37015	43,84	7

Таблица. Результаты тестирования антивирусных продуктов

Заключение

В ходе работы был проведен сравнительный анализ наиболее популярных существующих методик тестирования антивирусного ПО. Была разработана собственная

методика, учитывающая все недостатки предыдущих и обладающая рядом преимуществ, в первую очередь полной открытостью, адекватностью и универсальностью. Также на основе разработанной методологии было проведено сравнительное тестирование антивирусов наиболее крупных компаний в данной области IT-сферы.

Литература

1. Касперский Е. Вирусы и средства борьбы с ними. – М., 2005.
2. Сравнение антивирусов. – Режим доступа: http://svk.sanet.ru/articles/AntivirusDiffs/antivirusdiffs.htm
3. Опыт использования антивирусных программ. – Режим доступа: http://ambernic.nm.ru/antivir2.html
4. Andreas Clementi Anti-virus Comparative №5. On-demand detection of malicious software. – Режим доступа: http://ambernic.nm.ru/antivir2.html
5. Сравнение различных антивирусов на основе вероятностной оценки их качества. – Режим доступа: http://www.antivirus.ru/VirAnalizC.html
6. Сравнения средств защиты от вредоносных программ. – Режим доступа: http://www.anti-malware.ru/index.phtml?part=compare