УДК 004.492.4

ЛОЖНЫЕ СРАБАТЫВАНИЯ АНТИВИРУСНЫХ СРЕДСТВ

А. М. ТЕРЕНТЬЕВ,
кандидат технических наук,
ведущий научный сотрудник
E-mail: tam@cemi. rssi. ru
Центральный экономико-математический институт РАН

В статье затронуты вопросы ложных срабатываний антивирусных средств на примере отечественного пакета Doctor Web. Показана нарастающая актуальность рассматриваемого вопроса. Описан реальный пример, когда ложное срабатывание лишило компьютер работоспособности в Интернете. Показан порядок устранения ложных срабатываний на пакете DrWeb.

***Ключевые слова**: информационная безопасность, антивирусные средства, ложное срабатывание, операционная система.*

Программные средства борьбы с компьютерными вирусами, или антивирусные средства (далее – АВ-средства) известны давно. Когда-то написание вирусов являлось страстью одиночек, а их творения представляли широкий спектр разнообразных устремлений, от призыва легализовать марихуану (Legalize Marijuana) до зловредного эффекта «осыпания» букв на текстовом экране в MS-DOS. В настоящее время написание вирусов является развитой индустрией с оборотом в несколько миллиардов долларов в год, причем опасность заражения без использования АВ-средств при «прогулках» по Интернету является почти 100 %-ной.

С упомянутых давних времен и до настоящего момента АВ-средства существенно усложнились; также изменились их функции. Стандартным компонентом АВ-средств по-прежнему является ***сканер*** – программа сплошной или выборочной проверки файлов на HDD компьютера. Однако сравнительно новой и быстро развивающейся функцией сканера является предварительная проверка работающих процессов (прикладных и системных приложений, программ, библиотек), активных в оперативной памяти ПК перед началом проверки файлов на дисках. Эта совершенно необходимая функция исполняется современными АВ-средствами в привилегированном режиме и позволяет гарантировать, что дальнейшая проверка файлов ПК не приведет на самом деле к их заражению параллельно существующим вирусным процессом. Фактически работа сканера сводится к поиску уже зараженных файлов, что при нынешних скоростях распространения вирусов уже неэффективно. К настоящему времени сканеры не то чтобы устарели, просто их область применения изменилась: их стали вызывать тогда, когда нужно провести сплошную проверку заведомо зараженного ПК либо плановую проверку (например ежемесячную), а также для проверки сменных носителей – «флэшек», внешних HDD, CD, DVD и др.

Предупредить болезнь легче, чем лечить. Как и с человеком, профилактика заражения вирусами, работа «на опережение» с ПК становится гораздо более выгодной. Насущная потребность вызвала к жизни так называемые ***АВ-мониторы***. Это второй компонент стандартного АВ-пакета, который постоянно находится в оперативной памяти во все время работы пользователя и по некоторому алгоритму выборочно проверяет на вирусы те или иные файлы ПК.

Проверять все файлы, с которыми исполняется работа, крайне неэффективно: при этом полезная работа ПК замедлится в несколько раз. К настоящему моменту известны миллионы компьютерных вирусов, а проверять все файлы на миллионы сигнатур означает, по сути, практически блокировать работу ПК. Среди различных алгоритмов проверки, приме-

няемых в разных АВ-средствах, типовым является проверка всех загружаемых на исполнение модулей плюс проверка всех записываемых на ПК файлов. При использовании многоядерных процессоров и достаточного объема оперативной памяти (2–4 Гб) замедление от таких проверок наблюдается не более чем на 30%.

Полноты ради следует отметить, что описанными двумя компонентами современный АВ-пакет не исчерпывается. В развитых АВ-средствах обязательно присутствует проверка на вирусы отправляемой и принимаемой электронной почты, фаерволы, а с недавнего времени и проверка всего принимаемого контента просматриваемых Интернет-сайтов (например, в пакетах от Doctor Web серии Security Suite). Подробное рассмотрение этих функций выходит за рамки данной работы.

В отечественной печати и Интернете широко обсуждаются сравнительные характеристики различных АВ-средств, причем акцент делается на скорость проверки. Такой подход представляется излишне легковесным, поскольку скорость проверки зависит от числа хранимых вирусных сигнатур и, стало быть, вступает в противоречие с полнотой обнаружения вирусов. Представляется интересным обсудить другое свойство АВ-средств, такую крайне неприятную характеристику, как ***ложные срабатывания***.

Проверка любого файла любым АВ-средством на наличие известных вирусов состоит в сравнении по некоторому алгоритму кода проверяемого файла с миллионами так называемых ***сигнатур*** – хранимых образов известных вирусных кодов. Алгоритм проверки каждый разработчик сохраняет в секрете, как, собственно, и способ сохранения сигнатур в своих антивирусных базах, поскольку от этого сильно зависит скорость проверки. Естественно, что при недостаточной длине сигнатуры за вирус может быть принята вполне безобидная программа. В конкурентной борьбе за скорость, к сожалению, ряд вендоров старается использовать сокращенные или недостаточные сигнатуры, что и приводит к ложным срабатываниям.

Вообще говоря, вопрос ложных срабатываний стоял с самого начала у практически каждого АВ-средства. Оставляя в стороне такие анекдотические случаи, как принятие за вирус АВ-программой Avira собственных файлов после приема антивирусного дополнения от 27.10.2011, следует сказать, что на ложных срабатываниях отметились даже самые громкие имена, такие как Microsoft Security Essentials, который вдруг стал распознавать популярный браузер Google Chrome как троянское приложение PWS:Win32/Zbot. Автору известен случай с антивирусом «Doctor Web» (далее – DrWeb), который еще в самом начале своего существования упорно норовил принять за вирус программы автора данной работы, сгенерированные в MS-DOS компилятором TurboBasic.

Так случилось, что автор данной статьи исторически связан с АВ-средством DrWeb, который заслуженно известен как одно из двух отечественных лидирующих антивирусных средств. В варианте оригинальной, разработанной в ЦЭМИ РАН корпоративной поддержки серия пакетов DrWeb используется в ЦЭМИ РАН постоянно с 1999 г. Во время подготовки данной работы пакеты «***DrWeb для файловых Windows-серверов 6.0***», «***DrWeb для рабочих станций 5.0***», «***DrWeb для рабочих станций 6.0 Security Suite x86***» и «***DrWeb для рабочих станций 6.0 Security Suite x64***» постоянно используются на более чем 170 вычислительных установках института [1, 2]. Автору неплохо известны упомянутые пакеты и их предшественники, с самого начала презентации пакетов серии DrWeb и до настоящего времени он является их активным и последовательным сторонником [10–13 и др.]. Поэтому естественно, что рассмотрение таких девиаций, как ложные срабатывания, автору удобно провести именно на примере этих пакетов.

Наиболее опасны ложные срабатывания именно на мониторах, поскольку если при сканировании можно задать режим запроса на лечение, то в мониторах DrWeb версий 5.0 и 6.0 такой возможности нет, можно задать только рекомендуемую реакцию, каковой по умолчанию является *«Вылечить»,* что применительно к пакетам DrWeb означает приказ *удалить* неизлечимые модули.

Антивирусная служба ЦЭМИ РАН за многолетнюю историю эксплуатации антивирусных пакетов DrWeb не раз отмечала ложные срабатывания компонентов пакета на EXE-модулях. За все предшествующие годы (главным образом на ПК автора) это относилось к продукции различных компиляторов с алгоритмических языков PowerBASIC [3], продуцирующих как консольные, так и оконные (GUI) Windows-приложения. Необходимо отметить, что вопреки распространенному среди непрофессионалов мнению о примитивности PowerBASIC эта серия языковых компиляторов уже давно с

появлением TurboBASIC (несколько десятилетий назад) отошла от первого интерпретатора с таким базовым названием, причем в настоящее время она представляет собой серию мощных оптимизирующих профессиональных пакетов с развитыми подключаемыми библиотеками. В частности, возможность прямого программирования расширенными языковыми средствами на компиляторах ***PowerBASIC for Windows*** множества функций, специфичных для GUI-приложений операционной системы Microsoft Windows, а также возможность самостоятельно определять средствами языка непосредственно точки входа и параметры Windows API при сохранении высоты семантического класса языка позволяет значительно ускорить построение необходимых модулей (особенно расчетного характера) по сравнению с такими языками, как C и C++ [14–16].

К сожалению, эти же развитые особенности указанных компиляторов, видимо, и продуцировали время от времени, примерно раз в несколько лет, появление ложных срабатываний на пакетах DrWeb. Типичным примером является ложная реакция на тестовую программу автора, обнаруживающую саму себя среди прочих приложений по списку процессов с использованием входа ***GetWindowThreadProcessId*** в конце 2008 г. [4]. Программа была результатом компилятора ***PowerBASIC for Windows 8.04***.

Забавно, что одним из рекламных слоганов, используемых ООО «Doctor Web» как раз в то время, был ***«Лечим то, что другие даже не видят»…***

Однако случались и ложные срабатывания DrWeb на других модулях. Так, в марте 2008 г. DrWeb обнаружил «вирус» на фирменном CD в MSDN Library, подаренном автору Д. Н. Лозинским еще в 2003 г. [5].

Другой случай ложного срабатывания АВ-средств «Doctor Web» был отмечен в феврале 2010 г., когда за вирус посчитали внедряемый код компании SpyLog [8].

Приведенные случаи, безусловно, являлись единичными до 2012 г., когда ложные срабатывания стали происходить значительно чаще. Так, в июне 2012 г. появилось сразу 2 ложных срабатывания с диагностированием вирусов ***BackDoor. Tdss. 7916*** и ***BackDoor. Tdss. 7742*** в продукциях компилятора ***PowerBASIC for Windows 9.05***. Внезапно для автора при тестовых запусках был удален целый ряд демонстрационных файлов, входящих в дистрибутив-поставку компилятора [9]. В этот раз реакция последовала довольно быстро, менее чем через двое суток проблема была решена (конечно, все утерянные файлы пришлось перетранслировать из исходных текстов заново).

Далее, 21.07.2012 вирусы были обнаружены в файлах, содержащихся в кэшах Java версий 6.0/5 и 6.0/33 и пришедших вместе с обновлением версий. В этом случае Антивирусная лаборатория DrWeb вынесла заключение о вредоносности одного из указанных файлов [6], в чем автор данной статьи имеет все основания сомневаться: со времени нахождения на его ПК модуля, входящего в поставку Java 6.0/5, прошло несколько лет, причем никаких странных или непонятных действий за этим ПК замечено не было ни автором, ни работающим сетевым мониторингом [15], ни граничным маршрутизатором корпоративной сети института Cisco-7206. К сожалению, в своем ответе при вынесении положительного заключения о вредоносности данных эксплойтов служба техподдержки DrWeb не указала ни тип вредоносности, ни метод распространения, поэтому автор оставляет за собой право сомневаться в вынесенном вердикте.

Апофеозом ложных срабатываний автор считает случай, когда вирус был обнаружен в библиотеке (DLL) драйвера сетевого адаптера (рис. 1, 2)[1].

Ситуация стала очевидной следующим образом. После выхода автора из отпуска при включении рабочего ПК стало ясно, что он вдруг перестал «видеть» Интернет и всю локальную сеть. После многочасовой проверки всех физических соединений, температурного режима[2] процессора и материнской платы, проверки сообщений сетевого мониторинга за месяц отсутствия автора на рабочем месте и прочих манипуляций автор догадался запустить сканер на второй ОС, расположенной на том же ПК в другом разделе (подробнее см. в [17]), долго не загружавшейся ранее и полностью идентичной пораженной ОС. К удивлению, вирусом ***Trojan. Downloader6.46693*** оказался «заражен»

[1] Автор считает необходимым в ключевом примере привести «скрины» вместо ссылок после странной реакции руководства ООО «Doctor Web» на критические замечания автора, опубликованные на его сайте 15.03.2008 [12]. Руководство отдало приказ удалить со своих серверов ссылки на реальные, зафиксированные службой техподдержки и уже подтвержденные обращения автора (тикеты) по поводу многочисленных ошибок в новой тогда версии 4.44.

[2] В практике автора летом 2012 г. был случай, когда перегрев материнской платы из-за остановки кулера в блоке питания ничем иным на работе сервера не отразился, кроме нарушения сетевого соединения по одному из сетевых адаптеров.

Запрос 8DQM-0724 / Действие 3898044

Дата / время	28.08 04:54:26
Кто	Терентьев Александр Макарович
Действие, Статус запроса	Открытие, Новый
Информация	

Уважаемые господа!
На моём рабочем ПК внезапно после выхода из отпуска прекратилась связь с Интернетом. Проверка утилитой CureIt выявила файл, якобы заражённый Trojan.Downloader6.46693, прикреплённый к данному письму. То же показывает и DrWeb6.0SS. Подозреваю, что данный файл входит в комплект стандартных драйверов сетевого адаптера Realtek и срабатывание ложное. Очень прошу проверить актуальность срабатывания.
С уважением, Александр Терентьев

Цель использования: Зашита рабочих компьютеров/ноутбуков, не объединенных в сеть
Операционная система: Windows
Выбранный продукт: Dr.Web для защиты рабочих станций Windows
Серийный номер/номер лицензионного ключевого файла: UA85-TRX3-YRS3-GTLY

Организация: ЦЭМИ РАН – Центральный экономико-математический институт РАН
Должность: Рук.Антивирусной службы
Контактный телефон:

Присоединённые файлы:
Rt1CPAPI.dll (140K)

Рис. 1. Обращение в службу технической поддержки DrWeb по драйверу сетевой карты

Запрос 8DQM-0724 / Действие 3899840

Дата / время	28.08 20:22:32
Кто	Александр Бролин, служба технической поддержки
Действие, Статус запроса	Доп. информация, Ожидание ответа пользователя
Информация	

Срабатывание признано ложным, ошибка исправлена.
Благодарим за сотрудничество.

С уважением, Александр Бролин.
Служба технической поддержки компании "Доктор Веб".

Рис. 2. Ответ службы технической поддержки DrWeb по драйверу сетевой карты

файл RtlCPAPI. dll от 2006 г. (когда подобных вирусов вообще не было и в помине!), являющийся библиотекой драйвера сетевого адаптера «NVIDIA nForce Networking Controller».

С этого момента ситуация прояснилась: при исполнении начальной загрузки ОС монитор DrWeb заблокировал все обращения к этой библиотеке, а все сетевые функции ПК оказались бездействующими. Некоторую трудность представило общение с техподдержкой DrWeb (пришлось делать это с другого ПК), а после подтверждения ложности срабатывания проведение восстановления последних обновлений пакета «***DrWeb для рабочих станций 6.0 Security Suite x86***» вручную на пораженном ПК путем переноса последних файлов с соответствующей области Антивирусного сервера через «флэшку» во все 3 необходимых каталога. Разумеется, оказалось необходимым также восстановить удаленный файл, взяв его из другой ОС того же ПК.

Существенным в данном случае оказалась бы установка монитора не лечить или удалять бездумно все файлы, которые он сочтет вредоносными, а *перемещать в карантин*, благодаря чему файл, вызвавший ложное срабатывание, остался бы физически доступен на компьютере. К сожалению, до описанного момента такие установки автор на своем ПК не использовал. Да и кто знает, на что обратит свое внимание антивирусный пакет при следующем появлении ложного срабатывания – быть может, на какую-то часть самой ОС… В этом случае перемещение в карантин может заблокировать последующий запуск уже самой ОС.

При подготовке данной статьи обнаружилось, что пакет «***DrWeb для рабочих станций 6.0 Security Suite x86***» выдает еще одно срабатывание на EXE-модуле, продуцированном компилятором ***PowerBASIC for Windows 9.05***. На этот раз диагностирован ***BackDoor. CyberGate. 1*** в одном из примеров из поставки компилятора, демонстрирующем работу с панелью инструментов и ICO-файлами. Оно, конечно же, также было признано ложным [7].

Изложенное показывает, что наряду с реальными антивирусными угрозами опасность представляют также такие явления, когда антивирусные средства объявляют нормальные файлы на ПК зараженными. Эвфемизм «ложное срабатывание», используемый ведущими разработчиками АВ-средств, не раскрывает подлинной опасности этих явлений для пользователя. К сожалению, как видно на примерах срабатываний DrWeb только на одном компьютере, подобные явления понемногу превращаются в повседневность, существенно снижая доверие к хорошим антивирусным средствам.

Устранение ложных срабатываний на пакете DrWeb исполняется следующим образом. В антивирусной лаборатории DrWeb исследуется присланный образец. Если срабатывание признано ложным, то отыскивается то конкретное дополнение к антивирусным базам, которое содержит послужившую причиной ложной реакции сигнатуру вируса. Далее сигнатура уточняется, а измененное антивирусное обновление рассылается пользователям с новой датой. Так вот, поскольку на Антивирусном сайте ЦЭМИ РАН ведется статистика измененных обновлений, то можно подсчитать, что за полгода размер доли перевыпусков ранних обновлений – порядка 5 %.

С появлением описанной тенденции пользователям следует более критично относиться к сообщениям АВ-средств о выявлении вирусов, особенно в системном программном обеспечении. В случае, когда пользователь недостаточно опытен в классификации системных файлов, настройку монитора АВ-средств следует выставлять на перемещение в карантин с откладыванием окончательного решения вопроса об удалении файла до консультации со специалистом в АВ-технологиях.

Список литературы

1. Интернет-ресурс «Антивирусный сайт ЦЭМИ РАН. Статистика. Установки и обновления DrWeb для рабочих станций». URL: http://av. cemi. rssi. ru/av/r51w. htm.

2. Интернет-ресурс «Антивирусный сайт ЦЭМИ РАН. Статистика. Установки и обновления DrWeb для серверов». URL: http://av. cemi. rssi. ru/av/r51s. htm.

3. Интернет-ресурс «PowerBASIC: Basic Compilers». URL: http://www. powerbasic. com.

4. Интернет-ресурс «Антивирусный сайт ЦЭМИ РАН. Новости. 25.12.2008. Итоги осени 2008 г.». URL: http://av. cemi. rssi. ru?1,59.

5. Интернет-ресурс «Антивирусный сайт ЦЭМИ РАН. Новости. 15.03.2008. Новости для пользователей Doctor Web». URL: http://av. cemi. rssi. ru?1,53.

6. Интернет-ресурс «Сайт DrWeb. Тикет 6BN7-0158». URL: https://support. drweb. com/process/?ticket=6BN7-0158.

7. Интернет-ресурс «Сайт DrWeb. Тикет 9WHF-0274». URL: https://support. drweb. com/process/?ticket=9WHF-0274.

8. Интернет-ресурс «Сайт DrWeb. Сообщение об устранении ложного срабатывания по счетчикам SpyLog.» URL: http://news. drweb. com/show/?i=937&c=5&p=0.

9. Интернет-ресурс «Сайт DrWeb. Тикет HBHU-0728». URL: https://support. drweb. com/process/?ticket=HBHU-0728.

10. *Терентьев А. М.* Противовирусная защита ПК в Windows 95/98/NT. М.: ЦЭМИ РАН, 1999.

11. *Терентьев А. М.* Антивирусная защита ПК в Windows 95/98/NT / Справочное пособие по антивирусным средствам ЗАО «ДиалогНаука». 2-е издание. М.: ОАО «Перспектива», 2000.

12. *Терентьев А. М., Львова А. С.* Технология антивирусной защиты сетевых ПК с использованием специализированного сервера и ПК-сателлита // Развитие и использование средств мониторинга и аудита. Вып. 1. Сборник статей под ред. А. М. Терентьева. М.: ЦЭМИ РАН, 2004. С. 47–59.

13. *Терентьев А. М.* Выбор адекватных средств информационной защиты персонального компьютера в России // Национальные интересы: приоритеты и безопасность. 2012. № 33. С. 37–42.

14. *Терентьев А. М.* Методы и средства наблюдения загрузки локальных вычислительных сетей на примере ЦЭМИ РАН. М.:ЦЭМИ РАН, 2001.

15. *Терентьев А. М.* Построение и развитие системы сетевого мониторинга // Развитие и использование средств сетевого мониторинга и аудита. Вып. 1. Сборник статей под ред. А. М. Терентьева. М.: ЦЭМИ РАН, 2004. С. 5–23.

16. *Терентьев А. М.* Консоль управления сетевыми коммутаторами Cisco // Развитие технологий и инструментальных средств информационной безопасности. Вып. 1. Сборник статей под ред. А. М. Терентьева. М.: ЦЭМИ РАН, 2010. С. 6–20.

17. *Терентьев А. М.* Антивирусное обеззараживание персональных компьютеров с помощью подключения сторонних операционных систем // Национальные интересы: приоритеты и безопасность. 2012. № 37. С. 45–51.