СПИСОК ЛИТЕРАТУРЫ

1. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.
2. *Bell D. E., LaPadula L. J.* Security Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-306, MITRE Corporation MTR-2997. Bedford MA, March 1976.
3. *Biba K. J* Integrity Consideration for Security Computer System. The MITRE Corp., Report MTR N3153 Revision 1, Electronic System Division, U.S. Air Force Systems Command, Technical Report ESD TR 76 372. Belford, Massachusetts, April 1977.
4. *Щеглов К. А., Щеглов А. Ю.* Защита от атак со стороны приложений, наделяемых вредоносными функциями. Модели контроля доступа // Вопросы защиты информации. 2012. Вып. 4 (99). С. 31—36.

Сведения об авторах

Константин Андреевич Щеглов — студент; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: schegl_70@mail.ru

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 23.12.13 г.

УДК 004.056

Т. А. МАРКИНА, А. Ю. ЩЕГЛОВ

МЕТОД ЗАЩИТЫ ОТ АТАК ТИПА DRIVE-BY-ЗАГРУЗКА

Рассмотрены атаки типа drive-by-загрузка, использующие скриптовые вредоносные программы. Предложен метод защиты от таких атак, заключающийся в запрете загрузки (установки) или запуска несанкционированных скриптов (программ), запрете запуска несанкционированных скриптов под видом санкционированных и запрете модификации санкционированных скриптов. Продемонстрирована реализация этого метода.

Ключевые слова: *вредоносные программы, скрипт, защита информации, drive-by-атака, антивирусная программа.*

Введение. Одним из наиболее распространенных методов заражения компьютеров вредоносными программами, по данным компании „Лаборатория Касперского“, являются drive-by-атаки [1]. Практически весь TOP 20 [1] детектируемых web-антивирусом объектов состоит из скриптовых вредоносных программ, которые принимают участие в таких атаках. Стоит отметить, что атаки типа drive-by используют только скриптовые вредоносные программы.

Общее количество сайтов, использующихся в данных атаках, к концу июня 2013 г., по данным лаборатории McAfee, превысило 74,7 млн, что соответствует 29 млн доменных имен. Наиболее критично то, что 96% вредоносных доменов используются для атак drive-by [2].

Описание атаки drive-by. Рассмотрим технологию атаки (рис. 1). Первое время злоумышленники, применявшие загрузки drive-by, создавали вредоносные сайты и, чтобы привлечь на них посетителей, использовали социальную инженерию. Такие web-страницы до сих пор остаются основным источником вредоносной сетевой активности. Однако в последнее время хакеры заражают вполне „законопослушные“ сайты, размещая на них скриптовые

эксплойты или код для переадресации запросов, что позволяет незаметно для пользователя запускать атаки через браузер. В ходе такой атаки вредоносная программа автоматически загружается на компьютер-жертву без уведомления. Используются три типа вредоносных программ: редиректоры, скриптовые загрузчики и эксплойты.

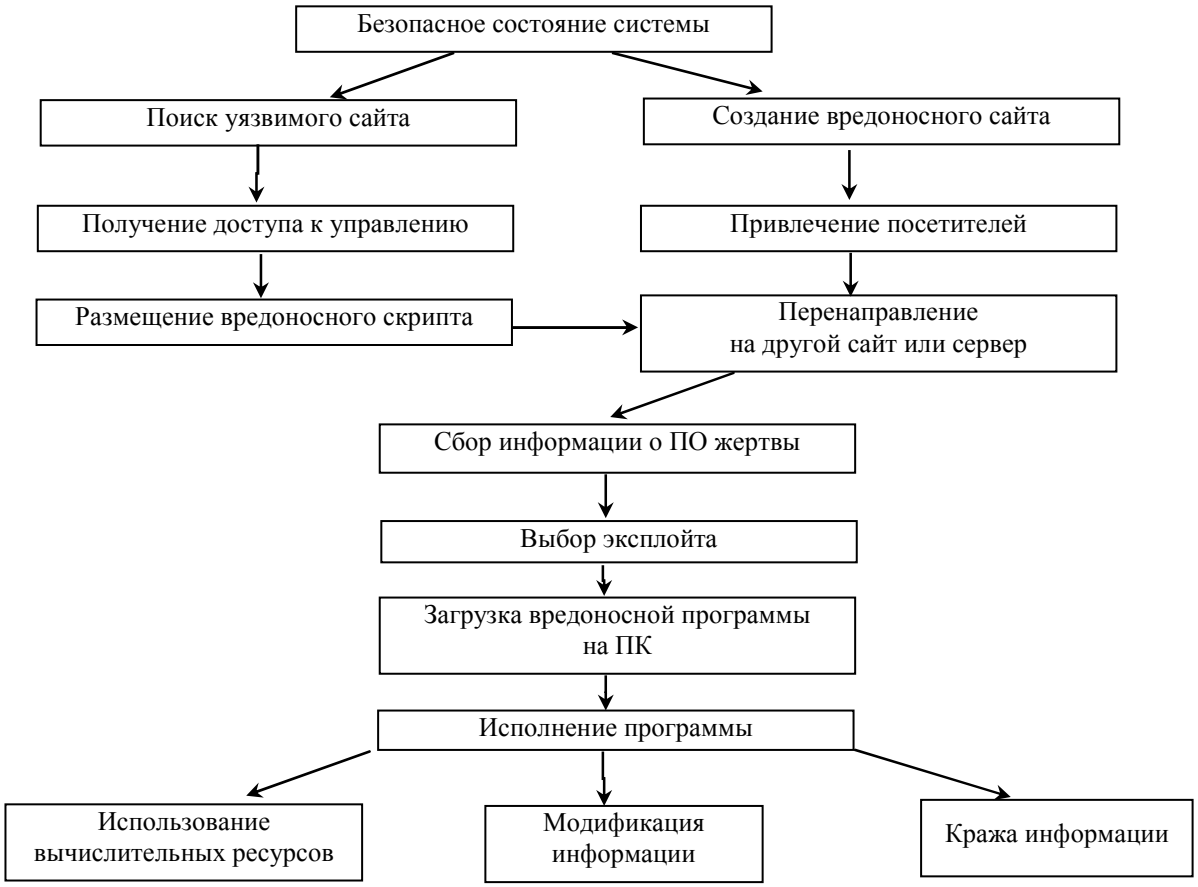

Рис. 1

Эксплойты, используемые при атаках drive-by, могут быть нацелены на незащищенные встраиваемые модули (плагины) web-браузера, уязвимости элементов управления ActiveX или средств защиты стороннего ПО [3]. Эксплойт выбирается на основании собранной информации о программах на компьютере жертвы (версия ОС, браузер и др.).

Сначала с зараженного сайта, в основном при помощи тэга <iframe>, происходит перенаправление пользователя на страницу, содержащую каскадные таблицы стилей (CSS) и вредоносный скриптовый загрузчик. Такой метод атаки затрудняет обнаружение вредоносных скриптов многими антивирусами и позволяет злоумышленникам избежать обнаружения загружаемых эксплойтов. Из рис. 1 видно, что прежде чем эксплойт будет загружен, может произойти любое количество переадресаций на другие сайты. В TOP 20 от компании „Лаборатория Касперского“ во втором квартале 2013 г. попали четыре редиректора: Trojan.Script.Iframer, Trojan.JS.FBook.q, Trojan.JS.Iframe.aeq и Trojan.JS.Redirector.xb.

Последние два при помощи тэга <iframe> перенаправляют пользователя на web-страницы злоумышленников. Первые два, помимо того что ими заражают легальные javascript-файлы, вызывают загрузку дополнительного скрипта JavaScript, это происходит, только если курсор двигается в пределах рабочего окна (т.е. событие „mousemove“ объекта „window“). Подобная техника применяется для обхода некоторых „песочниц“ и эмуляторов.

Далее скриптовые загрузчики Trojan-Downloader.Script.Generic, Trojan-Downloader.JS.JScript.cb, Trojan-Downloader.Win32.Generic, Trojan-Downloader.HTML.Iframe.ahs с зараженных web-страниц запускают эксплойт.

Загрузчики для хранения основных данных скрипта используют html-тэги. Скрипты первой группы — поле „alt“ тэга <img>, а второй — тэг . Для исполнения Java-эксплойтов загрузчики используют уязвимости в браузерах или pdf-ридерах.

Средства защиты. Защититься от атаки типа drive-by можно, используя различные антивирусные программы, имеющие модуль, который позволяет обнаруживать, что сайт заражен; утилиту Rozzle; сервис для проверки сайта на наличие заражения.

Первый способ защиты основан на сигнатурном поиске на web-сайтах и на поведенческом анализе.

Программа Rozzle является совместной разработкой компании Microsoft и Венского технического университета, представляющей собой виртуальную машину JavaScript, которая имитирует различные установки, предоставляя вредоносной программе различные пути для атаки. Иными словами, программа выдает себя за уязвимый браузер и эксплойт, с помощью которого происходит загрузка вредоносной программы, „попадающей в ловушку“. Средства поведенческого анализа смогли определить только 2,5 % угроз такого типа, в то время как Rozzle — 17,5 % [4].

Сервис проверки подозрительных сайтов действует следующим образом: следует ввести адрес проверяемого сайта в специальное поле и нажать кнопку „Проверить“.

Этот способ, как и первый, основывается на использовании существующих баз сигнатур, скорость составления которых значительно отстает от требуемой. Рассмотренные подходы неэффективны. Даже если считать, что пропускается всего 1 % (хотя на практике пропускается как минимум 80 % [4]), это может составить примерно 138 зараженных сайтов в день.

Предлагаемый метод защиты от атак типа drive-by-загрузки основан на разграничительной политике, но права доступа задаются не для каждого объекта доступа. В отличие от классической модели ОС семейства Windows, предлагается задавать права для пары „субъект доступа—объект доступа“. Субъект доступа включает в себя всех пользователей системы и все процессы. Главная особенность предлагаемого метода заключается в том, что объект доступа задается при помощи масок и исходя из типов файлов — для этого в ОС семейства Windows следует использовать расширения файлов (например, *.js). Для пары „субъект—объект“ задается запрет исполнения, записи, модификации, в том числе путем переименования существующих легальных скриптов, и переименования в разрешенные к запуску объекты, включая изменение расширений. В результате разрешается запуск только санкционированно установленных скриптов и предотвращается любая попытка создания новых скриптов на компьютере.

Реализация метода. Метод реализован на основе механизмов комплексного средства защиты информации „Панцирь+“ для ОС Microsoft Windows. При помощи масок назначаются объекты файловой системы, которые считаются исполняемыми, запрещаются их модификация и создание новых подобных объектов, в том числе переименованием. При помощи масок назначаются объекты файловой системы с расширениями *.js, *.vbs, *.php и др., которые являются файлами, написанными на скриптовых языках программирования. Запрещается их изменение и создание новых подобных объектов, в том числе путем переименования.

Для практической реализации метода был использован механизм контроля доступа к файлам. Был создан субъект доступа „Любой“ (рис. 2), учитывающий все процессы в данной системе. Затем назначались объекты файловой системы, являющиеся скриптовыми исполнимыми файлами. Наиболее распространенными на данный момент являются следующие файлы-скрипты с указанными расширениями: *.vbs и *.vbe (VBScript) задается как „*.vb*“; *.js и *.jse (JavaScript) задается как „*.js *“; *.wsf; *.wsh задается как „*.ws*“; *.scpt (AppleScript); *.php и *.asp., *.cgi (рис. 3).

После создания всех нужных объектов доступа устанавливаются разграничения к ним. Добавляя новое правило для выбранного объекта доступа, следует запретить все режимы доступа к нему. При этом следует фиксировать любой отказ в доступе (рис. 4).

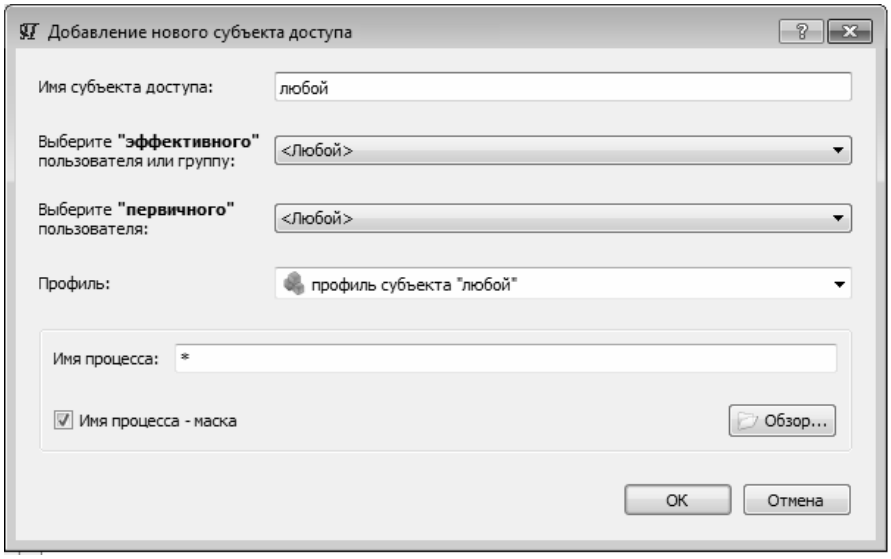

Рис. 2

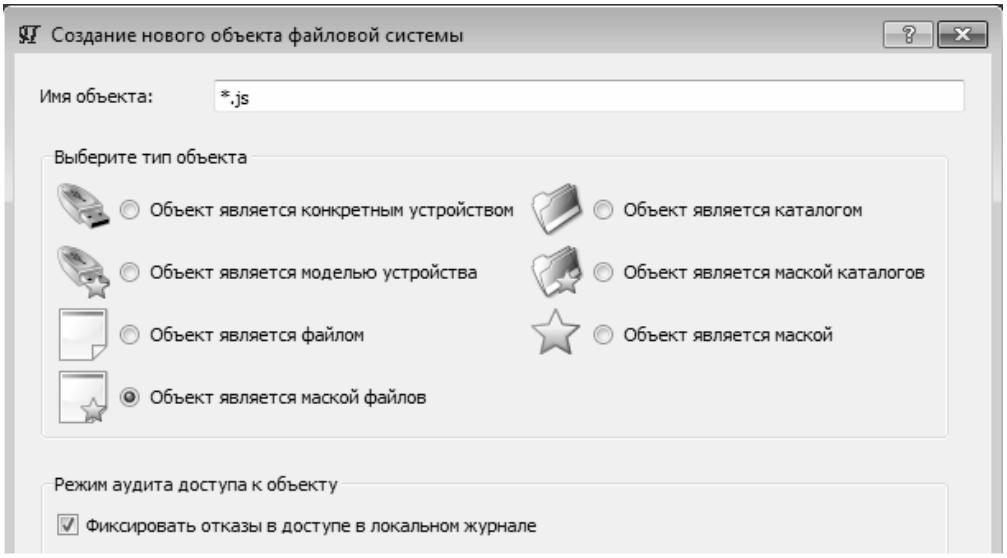

Рис. 3

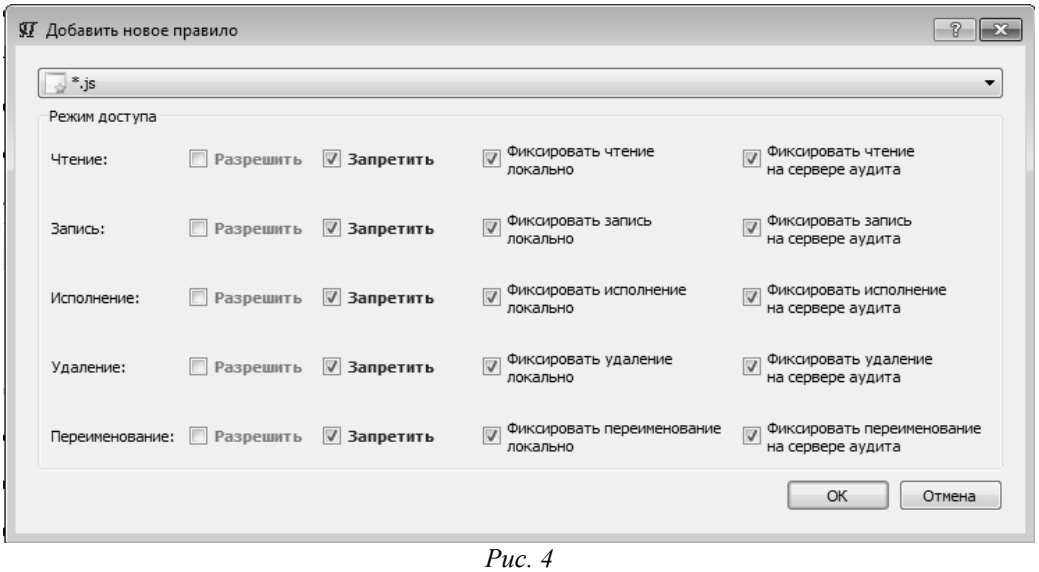

Рис. 4

Однако программы, которые присутствуют в системе и санкционированно исполняются, уязвимы. По-прежнему доступ для модификации, переименования и удаления остается открытым. Это, в свою очередь, является серьезной угрозой безопасности системы, так как критичные для пользователя программы могут быть удалены, испорчены или даже при помощи эксплойтов модифицированы таким образом, что станут выполнять вредоносные функции. Таким образом, следует обеспечить замкнутость среды. Для этого назначаются объекты файловой системы, необходимые для корректной работы операционной системы и требуемых программ, они находятся в системных каталогах %ProgramFiles% и %windir% (%systemroot%) и имеют расширения: *.exe, *.bat, *.com, *.config, *.dll, *.manifest, *.drv, *.fon, *.ttf, *.log, *.sys. После добавления объектов доступа создается правило для них, разрешающее чтение и исполнение, но запрещающее запись, удаление и переименование. При выполнении всех этих требований обеспечивается замкнутая среда исполнения. Теперь в системе возможен санкционированный запуск только необходимых программ, а вредоносное программное обеспечение, попавшее на компьютер тем или иным способом, не может быть запущено [5].

Для проверки эффективности предлагаемого метода следует посетить потенциально зараженные сайты. Предварительно необходимо настроить механизм аудита для всех созданных объектов на фиксацию всех запросов на запись, исполнение, удаление, переименование. После посещения зараженных страниц иди страниц с дополнительной рекламой в журнале управления доступом к файловой системе появятся сообщения о запрете записи и исполнения скриптовых вредоносных файлов.

Как видим, метод позволяет полностью защититься от несанкционированной записи и исполнения скриптовых вредоносных программ.

Заключение. Исследования показали, что атаки типа drive-by приводят к внедрению вредоносной программы на компьютер-жертву. Соответственно и защищаться нужно от загрузки файлов. Предлагаемый метод позволяет полностью защитить от таких атак, поскольку при любом способе установки вредоносного ПО в систему (использовались уязвимость в браузере или ошибка в Adobe Acrobat Reader) данная атака будет предотвращена.

Особенностью предлагаемого метода является то, что не сохраняются и не запускаются легальные скрипты с web-сайтов. Большинство из этих скриптов, как правило, предназначено для автозаполнения форм, рекламного баннера, загрузки дополнительной страницы с рекламой. Такие ограничения позволяют дополнительно защитить пользователя от получения ненужной рекламы.

СПИСОК ЛИТЕРАТУРЫ

1. *Масленников Д., Функ К.* Развитие информационных угроз во втором квартале 2013 года [Электронный ресурс]: <https://www.securelist.com/ru/analysis/208050807/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2013_goda#20>.

2. McAfee Threats Report: Second Quarter 2013 [Электронный ресурс]: <http://www.mcafee.com/ru/resources/reports/rp-quarterly-threat-q2-2013.pdf>.

3. *Шибаева Т. А.* Скриптовые вредоносные программы: способы внедрения и защита от них // Сб. тр. молодых ученых и сотрудников кафедры ВТ. 2012. Вып. 3. С. 78—80.

4. *Kolbitsch C., Livshits B., Zorn B., Seifert Ch.* Rozzle: De-Cloaking Internet Malware Microsoft Research [Электронный ресурс]: <http://research.microsoft.com/pubs/152601/rozzle-tr-10-25-2011.pdf>.

5. *Шибаева Т. А., Щеглов А. Ю., Оголюк А. А.* Защита от внедрения и запуска вредоносных программ // Вопросы защиты информации. 2011. Вып. 2 (93). С. 26—30.

Сведения об авторах

Татьяна Анатольевна Маркина — аспирант; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: tmark812@mail.ru

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 23.12.13 г.

УДК 004.627

А. А. Тропченко

МЕТОДЫ ПОВЫШЕНИЯ РОБАСТНОСТИ РАСПОЗНАВАНИЯ В МУЛЬТИМОДАЛЬНЫХ БИОМЕТРИЧЕСКИХ СИСТЕМАХ

Рассмотрены методы повышения робастности (устойчивости) распознавания в мультимодальных биометрических системах идентификации личности.

Ключевые слова: *распознавание личности, мультимодальные системы распознавания, объединение признаков, робастность.*

Для аутентификации и идентификации человека применяется биометрика — область знаний, использующая индивидуальные биологические особенности. Биометрические данные включают множество признаков (модальностей): отпечаток пальца, изображение лица, речь, геометрия кисти руки и ушной раковины, сетчатка глаза, подпись, динамика нажатия клавиш, походка, физиологические сигналы (электрокардиограмма) и т.д. У использования каждого признака есть свои преимущества и ограничения с точки зрения точности, устойчивости и удобства работы. Например, использование сетчатки обеспечивает высокую точность и устойчивость распознавания, но требует дорогого оборудования и существенных затрат времени.

Идентификация в динамике гораздо более сложная задача, особенно когда велико число зарегистрированных в системе пользователей. Динамические идентификационные системы на основе анализа аудиосигналов достигают высокой производительности, когда высоко отношение сигнал—шум (SNR) распознаваемого отрезка (текста). Однако устойчивость быстро ухудшается, когда SNR набора тестов уменьшается [1]. Для исследования устойчивости (робастности) распознавания личности при различных уровнях искажений был проведен ряд экспериментов.

На рис. 1 продемонстрировано последовательное снижение качества тестового изображения для аудиовизуальной базы данных XM2VTS, уровень вносимых искажений определяет параметр QF (Quality Factor).

QF=50 QF=14 QF=2

Рис. 1