УДК 351.864.1

УЧЕБНЫЙ ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ДЕМОНСТРАЦИИ ПРИНЦИПОВ РАБОТЫ ПРОГРАММНЫХ ЗАКЛАДОК И МЕТОДОВ ИХ ОБНАРУЖЕНИЯ

Русских А.Н., Минин И.В., Минин О.В.

ГОУ ВПО «Новосибирский государственный технический университет», Новосибирск, Россия (630092, г. Новосибирск, пр-т К. Маркса, 20), e-mail: russkikh.a@gmail.com

Разработан учебный программный комплекс, демонстрирующий возможности использования и методы поиска закладок в программном обеспечении. Исследования кода, содержащего закладку программы, позволили точно установить ее наличие в достаточно короткие сроки. Проверка проводилась как во время работы приложения, так и в случае если приложение было закрыто. Тесты показали, что в обоих случая поиск по ключевым словам дает одинаковые результаты как по скорости обнаружения, так и по количеству обнаруженных совпадений. По результатам исследований были сделаны выводы о возможных последствиях для информационной безопасности организаций при срабатывании закладок, а также описаны методы защиты. Также были разработаны рекомендации по противодействию и предотвращению чрезвычайных ситуаций, вызванных наличием и срабатыванием программных закладок.

Ключевые слова: закладка, программный комплекс, информационная безопасность.

TRAINING SOFTWARE FOR DEMONSTRATION OF THE PROGRAM BOOKMARKS PRINCIPLES AND METHODS OF THEIR DETECTION

Russkikh A.N., Minin I.V., Minin O.V.

Novosibirsk State Technical University, Novosibirsk, Russia (630092, Novosibirsk, K. Marx av., 20), e-mail: russkikh.a@gmail.com

A training software package that demonstrates the possibility of using bookmarks and search methods in the software was developed. Studies of code that contain the bookmark programs allowed it to ascertain the presence of a fairly short period of time. The test was conducted both at the time of application, and if the application was closed. Tests have shown that in both cases, a keyword search gives the same results as the rate of detection, and the number of matches were found. According to the research results were have made a conclusions about the possible consequences for the security organizations in the firing of bookmarks, as well as methods of protection are described. The same recommendations were developed to counter and prevent emergencies caused by the presence and the firing of the program tabs.

Key words: bookmark, software system, information security.

Введение

Целью настоящей работы являлось создание учебного программного комплекса для демонстрации принципов работы программных закладок и методов их обнаружения с целью обеспечения информационной безопасности предприятий, использующих внешнее (покупное) программное обеспечение. Учебный программный комплекс создавался в рамках дисциплин «Комплексное обеспечение информационной безопасности автоматизированных систем» и «Криптографические методы защиты информации» по специальности 090105.

Актуальность данной темы обусловлена все возрастающей угрозой внедрения т.н. вредоносных программных закладок. Так, вице-премьер Дмитрий Рогозин недавно (9.02.2012) заявил: «РФ должна сама производить ключевые элементы безопасности – мы будем способствовать тому, чтобы как можно быстрее достичь необходимого интеллектуального уровня в данном вопросе и начать производство элементной базы, иначе

мы будем на абсолютном крючке, и в момент "Ч", в особый период мы будем удивляться, почему у нас все отказало, начиная от мобильных телефонов и заканчивая светофорами». При этом, отметил он, в программное обеспечение, применяемое в сложном оборудовании, могут быть внедрены так называемые закладки, которые в случае необходимости могут сработать [2].

Вопрос об использовании закладок как в программном обеспечении, так и в аппаратной части современной техники не раз обсуждался специалистами в области информационной безопасности. Известный специалист в области ИБ и криптографии Брюс Шнайер в своем блоге http://www.schneier.com/blog/ заявил, что в Windows Vista SP1 содержался бэкдор в алгоритме генерации случайных чисел. При большой популярности и распространенности такого программного обеспечения наличие и возможность использования уязвимости представляет собой серьезную угрозу для многих предприятий и госучреждений [3]. «Это (закладки) элемент глобального мгновенного удара, смысл которого сводится к тому, чтобы, используя киберсети, разрушить институты военного и экономического управления страны противника, посеять хаос», – сказал Рогозин [2].

Последствия использования программных уязвимостей могут быть достаточно разнообразны. Сюда можно отнести:

- получение неавторизованного доступа с помощью удаленного проникновения в компьютер;
- блокирование системы или отдельной программы с помощью вредоносных скриптов;
- утечка паролей;
- копирование или изменение важных документов и файлов, нарушение коммерческой тайны организации;
- возможность выделения различной конфиденциальной информации сетевыми анализаторами.

Причины наличия люков в криптосистемах очевидны: разработчик хочет иметь контроль над обрабатываемой в его системе информацией и оставляет для себя возможность расшифровать ее, не зная ключа пользователя. Самыми известными примерами здесь являются AWARD BIOS (до версии 4.51PG) с его универсальным паролем «AWARD_SW» и СУБД Paradox фирмы Borland International, также имеющая «суперпароли» «jIGGAe» и «nx66ppx». Вице-премьер в своем выступлении также отметил: «Проблема не в хакерах каких-то неформальных, а в том, что закладки закладываются в ту элементную базу, от которой мы зависим, а мы ее используем в космосе, в атоме, еще неизвестно, что с нашими спутниками происходит, что там были за интересные фокусы» [2].

Описание программного комплекса

Для рассмотрения ситуации «как и где можно использовать вредоносную программную закладку» было написано специальное приложение. На примере этой программы будет продемонстрировано, что из себя представляет программная закладка, как она действует и каковы последствия ее использования.

Приложение CaesarSh представляет собой программный продукт, с графическим интерфейсом, написанный на современном языке программирования C#, в среде разработки Microsoft Visual Studio 2008, для операционной системы Windows 7.

Цель программы – продемонстрировать возможность использования программных закладок (специальных участков кода) в программном обеспечении и их влияние на работоспособность и безопасность компьютерной техники предприятий, использующих стороннее программное обеспечение.

Описание программы CaesarSh

Программа позволяет шифровать открытый текст по алгоритму Цезаря, пользователь может задать ключ (смещение) для шифрования. Различные тесты подтверждают, что программа работает корректно, и пользователь получает верные выходные данные.

Срабатывание программной закладки

При использовании программы в обычном режиме ничего непредвиденного не происходит. Введем в качестве входных данных открытый текст, состоящий из одного слова «exploit».

Программа также зашифровала текст, но при этом выполнился еще один участок кода, благодаря «особенным» входным данным. Так как введенная строка «CurStr» совпала со строкой «bug», последовало выполнение определенного участка кода.

Код приложения CaesarSh:

```
if (bug.CompareTo(CurStr) == 0)
// если строки равны (строка закладки и введенный окрытый текст)
{
MessageBox.Show("Закладка сработала"); // сообщение
using (Process process = Process.Start(@"E:\temp\del.bat")) // запускаем .bat // файл
(удаляет все файлы в указанной директории, и
// поддиректориях)

            {
  int pid = process.Id;
   }
```

}

Появилось всплывающее сообщение о том, что закладка сработала, а также в командной строке выполнился .bat файл del.bat, который удаляет все файлы в указанной папке и вложенный папках.

Код файла del.bat:

del /f /s /q E:\temp1

/f - удаляет все файлы, даже если у них установлен атрибут «только чтение»;

/s - удаляет файлы из всех подкаталогов;

/q - отключает запрос на подтверждение удаления файла;

E: - диск, на котором будут найдены и удалены файлы.

Во время тестового запуска были удалены специально скопированные файлы, но в качестве «цели» можно было указать домашнюю папку пользователя, папку Program Files или Windows.

В результате срабатывания закладки мы лишились всех файлов в папке temp1, также были удалены все файлы во вложенных папках.

Использование ПО для поиска закладки

Есть возможность найти программную закладку раньше, чем она, возможно, сработает. Консольное приложение Keywords написано на языке программирования C#, в среде разработки Microsoft Visual Studio 2008 для операционной системы Windows 7.

Поиск закладок программа Keywords будет осуществлять в графическом приложении CaesarSh, описанном ранее.

Описание программы Keywords

Программа Keywords просматривает папку по указанному пути и открывает все файлы с указанным расширением. Просматривая эти файлы, программа сравнивает их содержимое со своим входным параметром – строкой. Входной параметр Keywords – это строка, содержимое которой может совпадать кодом закладки в исследуемом приложении. Если программа находит такие же строки в файлах исследуемого приложения, она сообщает об этом и выводит имена файлов, где эти строки встречаются.

Код приложения Keywords:

```
string path = @"C:\Visual Studio2008\Projects\CaesarSh\CaesarSh\";
        // путь до проверяемой директории
string stext = "nnn";      // строка (ключевое слово), которое ищем в
  // "*.filetype"
DirectoryInfo di = newDirectoryInfo(path);
FileInfo[] files = di.GetFiles("*.cs"); // тип файлов, которые просматриваем
```

// на наличие закладки.

Для начала проверим все файлы с расширением «.cs» на наличие строки «nnn». После проверки программа сообщила, что во всех файлах с расширением «.cs» в проверяемой папке нет слова «nnn».

Еще раз проверим файлы с указанным ранее расширением на содержание строки «.bat». После проверки программа сообщила, что файл Form1.cs содержит строку «.bat», понятно, что в программе CaesarSh вызывается .bat файл, стоит еще проверить файлы этой программы.

Снова проверим файл Form1.cs, на этот раз будем искать строку «using (Process process = Process.Start». Проверка показала, что такая строка действительно присутствует в коде исследуемой программы. Имеет смысл предположить, что это строка служит для запуска некоторого процесса, например .bat файла.

Следующая проверка показывает, что программе Keywords удалось найти в файле Form1.cs строку «Закладка сработала», можно сделать вывод, что текст программы CaesarSh содержит специальные участки кода, которые необходимо изучить подробнее.

Программа Keywords может проверять любые типы файлов в указанной папке на наличие специальных строк. Можно проверить как файлы, содержащие код приложения, так и файлы ресурсов, содержащие входные параметры.

Выводы

Такая уязвимость в программном обеспечении, как закладки, может представлять серьезную угрозу как для страны в целом, так и для конкретных компаний и учреждений. Срабатывание программных закладок может быть инициировано злоумышленниками в самый неподходящий момент, и последствием от их использования может стать как потеря информации и прибыли компании, так и угроза национальной безопасности страны. На наш взгляд, для минимизации возможности наличия уязвимостей и закладок при использовании покупного программного обеспечения необходимо:

- использовать проверенное и имеющее сертификаты программное обеспечение;
- отдавать предпочтение программному обеспечению, имеющему открытый исходный код;
- производить резервное копирование важных файлов, документов и баз данных, чтобы иметь возможность быстро восстановить работу организации;
- создавать и использовать программные системы и сетевые решения, в которых бы учитывалась возможность вредоносного воздействия и возможность отключения пораженного участка;

- при возможности в критически важных проектах и решениях использовать «собственное» программное обеспечение.

Список литературы

1. Казарин О.В. Безопасность программного обеспечения компьютерных систем : монография. – М. : МГУЛ, 2003. – 212 с.
2. Колесов А. Безопасность ПО: кто кого боится? [Электронный ресурс] // Интернет журнал PCWEEK. Режим доступа: http://www.pcweek.ru/foss/blog/foss/1975.php (дата обращения: 21.03.2012).
3. Рогозин Д.О. Европа проутюжена американским катком [Электронный ресурс] // Голос России: государственная радиовещательная компания. – Новосибирск, 2012. – 9 фев. – Режим доступа: http://rus.ruvr.ru/2012/02/09/65682824.html (дата обращения: 17.03.2012).
4. Шевченко А. Технологии обнаружения вредоносного кода. Эволюция [Электронный ресурс] // Сетевая газета InfoSecurity. Режим доступа: http://www.infosecurity.ru/_gazeta/content/071109/article01.shtml (дата обращения: 20.03.2012).
5. Schneier B. Did NSA Put a Secret Backdoor in New Encryption Standart? / B. Schneier // [Electronic resource], 15 November, 2007. – Режим доступа: http://www.schneier.com/blog/archives/2007/12/dual_ec_drbg_ad.html http://www.schneier.com/essay-198.html (дата обращения: 17.03.2012).

Рецензенты

Гужов Владимир Иванович, д.т.н., профессор, декан АВТФ НГТУ, г. Новосибирск.

Воевода Александр Александрович, д.т.н., профессор НГТУ, г. Новосибирск.