ПРОГРАММНЫЕ ЗАКЛАДКИ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Прохоренко Т.Н.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

По мере развития средств защиты компьютерных систем развиваются и средства нападения. Злоумышленники-хакеры изобретают всё новые и новые атаки на различные элементы подсистем защиты компьютерных систем. Одной из наиболее опасных является атака защищённой системы посредством программных закладок.

Программная закладка– это скрытно внедрённая в защищенную систему программа, либо намеренно изменённый фрагмент программы, которая позволяет злоумышленнику осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты. То есть основное предназначение закладок – обеспечить несанкционированный доступ к конфиденциальной информации.

Основная опасность программных закладок заключается в том, что программная закладка, являясь частью защищённой системы, способна принимать активные меры по маскировке своего присутствия в системе. При внедрении в систему закладки в защищённой системе создаётся скрытый канал информационного обмена, который, как правило, остаётся незамеченным для администраторов системы в течение длительного времени. Практически все известные программные закладки, применявшиеся в разное время различными злоумышленниками, были выявлены либо из-за ошибок, допущенных при программировании закладки, либо же просто случайно.

Существуют три основные группы деструктивных действий, которые могут осуществляться программными закладками:

– копирование информации пользователя компьютерной системы (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов), находящейся в оперативной или внешней памяти этой системы, либо в памяти другой компьютерной системы, подключённой к ней через локальную или глобальную компьютерную сеть;

– изменение алгоритмов функционирования системных, прикладных и служебных программ (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям вне зависимости от правильности введённого пароля);

– навязывание определённых режимов работы (например, блокирование записи на диск при удалении информации, при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована хакером).

К наиболее известным моделям воздействия программных закладок на компьютеры относятся следующие виды:

1. *Модель «перехват»*. Программная закладка внедряется в постоянное запоминающее устройство, оперативную систему или прикладное программное обеспечение и сохраняет все или избранные фрагменты вводимой или выводимой информации в скрытой области локальной или удалённой внешней памяти прямого доступа. Объектом сохранения может быть клавиатурный ввод, документы, выводимые на принтер, или уничтожаемые файлы-документы.

2. *Модель «троянский конь»*. Закладка встраивается в постоянно используемое программное обеспечение и по некоторому активизирующему событию моделирует сбойную ситуацию на средствах хранения информации или в сети. Тем самым могут быть достигнуты две различные цели: парализована нормальная работа компьютерной системы,злоумышленник (например, под видом обслуживания или ремонта) может ознакомиться с имеющейся в системе или накопленной посредством использования модели «перехват» информацией.

3. *Модель «наблюдатель»*. Закладка встраивается в сетевое или телекоммуникационное программное обеспечение. Данное программное обеспечение, как правило, всегда активно, в результате чего программная закладка осуществляет контроль за процессами обработки информации на компьютере, установку и удаление закладок.

4. *Модель «компрометация»*. Закладка либо передаёт заданную злоумышленником информацию (например, клавиатурный ввод) в канал связи, либо сохраняет её, не полагаясь на гарантированную возможность последующего приёма или снятия.

5. *Модель «искажение или инициатор ошибок»*. Программная закладка искажает потоки данных, возникающие при работе прикладных программ (выходные потоки), либо искажает входные потоки информации, либо инициирует возникающие при работе прикладных программ ошибки.

6. *Модель «сборка мусора»*. В данном случае изучаются «остатки» информации. В случае применения программной закладки навязывается такой порядок работы, чтобы максимизировать количество остающихся фрагментов ценной информации. Злоумышленник получает либо данные фрагменты, используя закладки моделей 2 и 3, либо непосредственный доступ к компьютеру под видом ремонта или профилактики.

Наиболее эффективным методом защиты от программных закладок является использование организационных мер, к которым можно отнести следующие:

– минимизация времени работы в компьютерной системе с полномочиями администратора;

– создание специальной учётной записи пользователя компьютерной системы для выхода в сеть Интернет с минимальными полномочиями;

– аккуратное использование почтовых и офисных программ привилегированными пользователями (например, запрет доступа администратора к отдельным папкам и файлам).

Помимо организационных мер, немаловажным эффективным методом защиты от вредоносных программ является создание изолированной программной среды, обладающей следующими свойствами:

– установлена система BIOS, не содержащая программных закладок, операционная система проверена на наличие в ней закладок;

– достоверно установлена целостность модулей операционной системы и BIOS для данного сеанса работы пользователя;

– исключён запуск любых программ в данной программно-аппаратной среде, кроме проверенных;

– исключён запуск проверенных программ в каких-либо иных условиях, кроме перечисленных выше, т. е. вне изолированного компьютера.

Таким образом,самым распространённым способом внедрения программной закладки является внедрение с помощью сети Интернет.Программные закладки способны уничтожать или искажать информацию, нарушать сеансы работы. Они могут собирать информацию, которая отправляется злоумышленнику по системе электронной почты для анализа на предмет содержания ценной информации, такой как пароли или пользовательская информация.Для обеспечения безопасности своих документов и предохранения самого компьютера от программных закладок достаточно соблюдать ряд правил и мер предосторожности, однако много компьютеров оказываются заражёнными из-за элементарной неосведомленности пользователя. В соответствии с комплексным подходом к обеспечению информационной безопасности универсальных приёмов, сохраняющих постоянную эффективность, быть не может. Требуется тщательный анализ новой информации о типах программных закладок и способах их внедрения в компьютерную систему для выбора адекватных методов защиты.