Например, в отчёт «Инвойс» автоматически заполняются данные об отправителе, покупателе, грузополучателе, контейнер, номер, дата, данные о товаре (размеры, количество штук, объём, цена, сумма всего в долл. США). Вся остальная информация остаётся неизменной.

Таким образом, разработанная БД «Пиломатериалы» позволяет сотрудникам РУП «Белтаможсервис» автоматически заполнять пакет документов.

ПРОГРАММНЫЕ ЗАКЛАДКИ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Шорина А.А
Научный руководитель: ст. преподаватель Ковалькова И.А.
Беларусский национальный технический университет

Одним из самых распространенных на сегодня источником получения информации являются компьютерные сети. Они постепенно превратились в такую же повседневность, как и телевидение или телефон. Множество компаний имеют свои собственные официальные страницы в Internet, подразделения компаний используют компьютерные сети для оперативного обмена коммерческой информацией, тысячи рядовых граждан используют сеть для получения важных для них данных. Задача защиты информации, хранимой в компьютерных системах, от несанкционированного доступа (НСД), является весьма актуальной. Для решения этой задачи используется целый комплекс средств, включающий в себя технические, программно-аппаратные средства и административные меры защиты информации. По мере развития средств защиты компьютерных систем развиваются и средства нападения. Изобретают все новые и новые атаки на различные элементы подсистем защиты компьютерных систем. Одной из наиболее опасных является атака защищенной системы посредством программных закладок.

Программные закладки – это скрытные (недокументированные) возможности в программном и аппаратном обеспечении персональных компьютеров и периферийного оборудования, позволяющие осуществлять скрытый несанкционированный доступ к ресурсам системы (как правило, посредством локальной или глобальной сети). То есть основное предназначение закладок – обеспечить несанкционированный доступ к конфиденциальной информации.

Основная опасность программных закладок заключается в том, что, программная закладка, являясь частью защищенной системы, способна принимать активные меры по маскировке своего присутствия в системе.

При внедрении в систему закладки в защищенной системе создается скрытый канал информационного обмена, который, как правило, остается 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 чисто случайно.

Если программная закладка написана грамотно, то после того, как она внедрена в систему, обнаружить ее стандартными средствами администрирования очень трудно, поэтому она может функционировать неограниченно долгое время, – и на протяжении всего этого времени внедривший ее злоумышленник имеет практически неограниченный доступ к системным ресурсам.

Закладки могут наносить ущерб как отдельным пользователям и компаниям, так и целым государствам, например, ставя под угрозу обороноспособность страны.

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

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

– изменение алгоритмов функционирования системных, прикладных и служебных программ;

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

Программные закладки можно классифицировать **по методу их внедрения в компьютерную систему**:

– программно-аппаратные закладки, ассоциированные с аппаратными средствами компьютера (их средой обитания, как правило, является BIOS — набор программ, записанных в виде машинного кода в постоянном запоминающем устройстве — ПЗУ);

– загрузочные закладки, ассоциированные с программами начальной загрузки, которые располагаются в загрузочных секторах (из этих секторов в процессе выполнения начальной загрузки компьютер считывает программу, берущую на себя управление для последующей загрузки самой операционной системы);

– драйверные закладки, ассоциированные с драйверами (файлами, в которых содержится информация, необходимая операционной системе для управления подключенными к компьютеру периферийными устройствами);

– прикладные закладки, ассоциированные с прикладным программным обеспечением общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки);

– исполняемые закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаще всего эти модули представляют собой пакетные файлы, т. е. файлы, которые состоят из команд операционной системы, выполняемых одна за одной, как если бы их набирали на клавиатуре компьютера);

– закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек);

– замаскированные закладки, которые маскируются под программные средства оптимизации работы компьютера (файловые архиваторы, дисковые дефрагментаторы) или под программы игрового и развлекательного назначения.

Универсальным средством защиты от внедрения программных закладок является создание *изолированного* компьютера.

Компьютер называется изолированным, если выполнены следующие условия:

– в нем установлена система BIOS, не содержащая программных закладок;

– операционная система проверена на наличие в ней закладок;

– достоверно установлена неизменность BIOS и операционной системы для данного сеанса;

– на компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них закладок;

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

Можно ли «застраховать» свой компьютер от проникновения программных закладок? Стопроцентной защиты информационной системы от воздействия программных закладок не существует. Внедрение программной закладки в программную среду может произойти случайно: через сеть, со съемного носителя и другими способами. Программная закладка может быть внедрена в среду изначально, еще на стадии проектирования программного обеспечения. Закладки, внедренные на

стадии разработки программного обеспечения, не обнаруживаются вообще. Однако возможно снизить риск проникновения программных закладок в систему. Для этого следует устанавливать только сертифицированное программное обеспечение, запретить автоматическое обновление и установку файлов .dll неизвестного происхождения. Базовым способом защиты от проникновения программных закладок в компьютер является установка средств мониторинга процессов, происходящих в системе, сканеров, в основе которых вместо сигнатурного анализа применяются механизмы семантики и эвристики.

Литература

1. Анин, Б. Ю. «Защита компьютерной информации» / Б. Ю. Анин. - СПб.: БХВ-Петербург, 2000. - 384 с.

2. Каторин, Ю. Ф. «Большая энциклопедия промышленного шпионажа» / Ю.Ф. Каторин, Е.В. Куренков , А.В. Лысов , А. Н. Остапенко. — СПб.: 000 «Издательство Полигон», 2000. — 896 с.

3. Казарин, О.В. «Безопасность программного обеспечения компьютерных систем» / О. В. Казарин – М.: МГУЛ, 2003. - 212 с.

4. Соколов, А. Степанюк О. «Защита от компьютерного терроризма» / А. Соколов , О. Степанюк – СПб.: БХВ-Петербург, Арлит, 2002. – 496с.

КОММЕРЧЕСКИЕ ТАМОЖЕННЫЕ УСЛУГИ

Яковец А.Г.
Научный руководитель: ст. преподаватель Лабкович О.Н.,
Белорусский национальный технический университет

Международная торговля услугами не является новым явлением. В условиях развития внешней торговли, расширения сотрудничества с международными экономическими и финансовыми институтами появилась острая необходимость в освоении новых путей повышения качества и эффективности таможенного обслуживания в целях максимального содействия развитию внешнеторговой деятельности.

Таможенное администрирование, являясь неотъемлемой частью системы государственного управления внешнеторговой деятельностью. Таможенные услуги проявляются как особая форма экономической деятельности, которая может способствовать созданию благоприятных условий, либо устанавливает определенные барьеры для осуществления внешнеторговой деятельности.