Лекция 16. Защита от программных закладок и несанкционированного копирования

1. Программные закладки и защита от них.
2. Принципы построения и состав систем защиты от несанкционированного копирования.
3. Методы защиты от копирования инсталляционных дисков и установленного ПО.

Методы внедрения программных закладок

1. Маскировка под «полезное» ПО.
2. Маскировка под модуль расширения возможностей программной среды (драйвер, DLL).
3. Подмена уже установленного ПО.
4. Прямое ассоциирование с уже установленным ПО.
5. Косвенное ассоциирование с ПО ядра ОС в оперативной памяти.

Причины, способствующие внедрению программных закладок

- Разрешение пользователю доступа по записи к критичному системному ресурсу.
- Сохранение (установка) уязвимой сетевой службы.
- Оставление незаблокированной консоли администратора.
- Требования высокопоставленных пользователей и т.д.

Признаки внедрения программных закладок

- Изменение конфигурационных файлов ОС (например, реестра Windows) для обеспечения автозапуска закладки при загрузке ОС.
- Использование для связи с нарушителем протокола TCP/IP с большим номером порта.
- Создание после своей загрузки отдельного процесса.
- Отсутствие длительное время после загрузки активных действий.

Признаки внедрения программных закладок

- Оставление следов в файле аудита и др.

Технология «руткитов»

- Изначально словом «руткит» обозначался набор инструментов, позволяющий нарушителю входить в систему таким образом, чтобы системный администратор не мог его видеть, а система - регистрировать.
- Руткиты могут применяться в коммерческих продуктах для защиты от несанкционированного копирования.

Технология «руткитов»

- Практически все современные версии руткитов могут скрывать от пользователя файлы, папки и параметры реестра, работающие программы, системные службы, драйверы и сетевые соединения.
- В основе функционирования руткитов лежит модификация данных и кода программы в памяти операционной системы.

Виды руткитов

- работающие на уровне ядра (Kernel Level, или KLT);
- функционирующие на пользовательском уровне (User Level).

Защита от руткитов

- Существующие сегодня специализированные программы, предназначенные для обнаружения руткитов, и традиционные антивирусы не дают стопроцентной гарантии безопасности.
- Обладая исходным кодом этих программ, можно создать любые модификации руткитов или включить часть кода в любую шпионскую программу.
- Главная цель руткитов не прочно закрепиться в системе, а проникнуть в нее.

Предотвращение внедрения программных закладок

Организационные меры:

- Минимизация времени работы в системе с полномочиями администратора.
- Создание отдельной учетной записи для работы в Интернете (с минимальными правами: запуск браузера и сохранение файлов в выделенной папке).
- Осмотрительная работа с почтовыми и офисными программами и др.

Система защиты от копирования

Комплекс программных (программно-аппаратных) средств, обеспечивающих затруднение нелегального распространения, использования и (или) изменения программных продуктов.

Нелегально – без согласия владельца авторских прав. Нелегальное изменение – для того, чтобы измененный продукт не попадал по действие законодательства о защите авторских прав.

Надежность системы защиты от копирования

Способность противостоять попыткам проникновения в алгоритм ее работы и обхода механизмов защиты.

Любая система защиты от копирования может быть раскрыта за конечное время (т.к. ее команды в момент своего исполнения присутствуют в оперативной памяти в открытом виде).

Надежность системы защиты определяется надежностью ее слабейшего звена.

Принципы создания системы защиты от копирования

1. Учет условий распространения защищаемых программных продуктов.
2. Учет особенностей защищаемых программных продуктов.
3. Учет особенностей пользователей защищаемых программных продуктов.
4. Оценка возможных потерь от снятия защиты.

Принципы создания системы защиты от копирования

5. Учет особенностей «взломщиков».
6. Постоянное обновление применяемых средств защиты.

Условия распространения программных продуктов

1. Распространение на инсталляционных дисках (установка продукта пользователем). Возможные угрозы:

- копирование инсталляционных дисков;
- изучение работы системы защиты (обычно при помощи отладчиков и декомпиляторов или дизассемблеров);
- перенос установленного продукта на другие компьютеры;
- моделирование работы системы защиты и изготовление тождественного варианта инсталляционного диска

Условия распространения программных продуктов

2. Установка программного продукта представителем его изготовителя или продавца. Возможные угрозы:
   - перенос установленного продукта на другие компьютеры;
   - изучение работы системы защиты.
3. Покупатели программного продукта не заинтересованы в его нелегальном распространении. Возможная угроза:
   - несанкционированное использование продукта.

Особенности программных продуктов

- Предполагаемый тираж.
- Розничная и оптовая цена.
- Частота обновления версий.
- Специализированность и сложность.
- Уровень сервиса для легальных покупателей.
- Скидки при обновлении продукта (upgrade).

Особенности пользователей программных продуктов

- Наличие (возможность привлечения) квалифицированных программистов для снятия защиты.
- Возможность реального применения юридических санкций к нарушителям законодательства о защите авторских прав.

Особенности «взломщиков»

- Хорошее знание системного программирования и операционных систем.
- Более слабая подготовка в области дискретной математики, криптографии и других математических дисциплин.

Универсальные и специализированные системы защиты

Готовые решения:

- менее надежны;
- могут быть несовместимы с защищаемым программным продуктом.

Специализированная система:

- более дорогая.

Требования к системе защиты от копирования

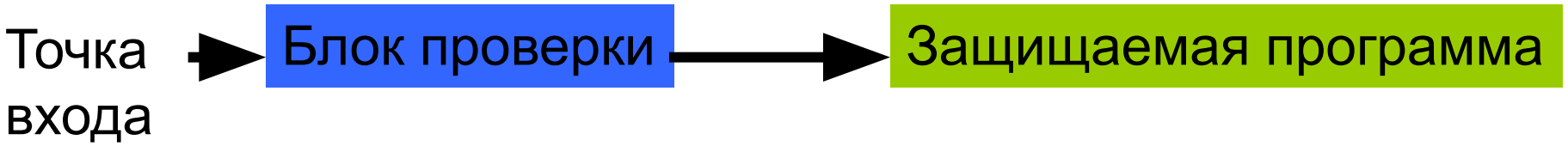
- Некопируемость инсталляционных дисков стандартными средствами операционных систем.
- Невозможность применения стандартных отладчиков.
- Некорректное дизассемблирование (декомпиляция) стандартными средствами.
- Сложность изучения структуры ключевой информации, используемой при проверке легальности запуска программы.

Типовая структура системы защиты от копирования

1. Блок проверки ключевой информации.
2. Блок защиты программы от изучения (противодействия отладчикам и дизассемблерам/декомпиляторам).
3. Блок согласования с защищаемыми структурами (обеспечения правильной работы защищаемых программ и правильного расшифрования защищаемых данных при легальном использовании).

Реализация блока проверки ключевой информации

1. В виде отдельного модуля.



Реализация блока проверки ключевой информации

2. В виде «навесного» модуля (по технологии компьютерного вируса).

Реализация блока проверки ключевой информации

3. В виде нескольких внутренних функций проверки (ФП).

Защита инсталляционных дисков

Создание некопируемой метки (совокупности информационных признаков носителя, существенно изменяющихся при его копировании).

Виды некопируемой метки:

- программная (логическая);
- физическая.

Основные приемы нанесения программной метки

1. Изменение стандартного формата диска.
2. Привязка к временным характеристикам чтения и(или) записи диска.
3. Комбинация нескольких приемов (в том числе в сочетании с шифрованием данных на диске).

Особенности файловой системы CDFS

Каждый файл имеет две основные характеристики:

- номер начального сектора;
- длина в байтах.

Способы нанесение программной метки на CD

1. Увеличение значения длины файла (его последний сектор должен находиться за пределами диска). Для преодоления такой защиты нарушителю достаточно задать размер считываемого файла таким, чтобы он помещался на CD, а после копирования на файла на жесткий иск отбросить ненужную информацию.

Способы нанесение программной метки на CD

2. Изменение номера начального сектора файла (уменьшение или увеличение его фактического размера).
3. Сочетание двух рассмотренных выше способов.

Если правильные значения номера начального сектора и длины файла будут храниться в программе установки, нарушитель может их выделить среди других констант программы.

Способы нанесение программной метки на CD

4. Использование временных характеристик чтения информации с диска. Недостатки этого способа:

- вероятностный характер результатов проверки;
- зависимость временных характеристик не только от конкретного носителя, но и от используемого для чтения диска привода.

Нанесение физической метки

Искусственное (механическое или с помощью лазера) создание дефектов на поверхности диска, проверка и сохранение их местоположения. При считывании данных с этого места при установке программного продукта проверяется возникновение сообщения об ошибке чтения. Адрес дефектного сектора может использоваться для получения регистрационного кода, который должен ввести пользователь в процессе установки программного продукта.

Защита от копирования установленного программного обеспечения

Обычный порядок установки защищенного программного продукта:

1. Запуск программы установки с инсталляционного диска и проверка ключевой информации (например, некопируемой метки).
2. При успехе проверки получение от пользователя сведений о месте установки программы и другой необходимой информации.

Установка защищенного программного продукта

3. Копирование файлов на жесткий диск.
4. Обновление реестра ОС.
5. Обновление меню Пуск | Программы.
6. Создание ярлыка на Рабочем столе.
7. Сбор и сохранение ключевой информации о параметрах компьютера и учетной записи пользователя (возможно с вычислением электронной цифровой подписи пользователя под собранной информацией).

Характеристики компьютера и пользователя

- Имя учетной записи пользователя.
- Имя компьютера.
- Серийные номера жесткого диска и других аппаратных устройств.
- Параметры BIOS (номер версии и дата создания).
- Объем оперативной памяти и раздела жесткого диска.
- Состав дисковых устройств.

Характеристики компьютера и пользователя

- Параметры устройств ввода-вывода (клавиатуры, мыши, монитора, принтера).
- Версии операционной и файловой системы.

Эти сведения могут быть собраны с помощью функций из набора Windows API или непосредственным чтением параметров из реестра ОС.

- Индивидуальные спецификации функций аппаратного устройства (обычно USB-ключа), поставляемого вместе с программным продуктом.

Проверка ключевой информации при запуске после установки

1. Сбор характеристик, аналогичных тем, что были использованы при установке.
2. Чтение сохраненных при установке характеристик (эталонных).
3. Сравнение вновь собранных и эталонных характеристик (возможно с проверкой электронной цифровой подписи пользователя).