Системы защиты программных продуктов, распространяемых на CD, от несанкционированного копирования.

Согласно исследованию, проведенному Business Software Alliance и Software Publishers Association, 4 из 10 деловых приложений, инсталлированных во всем мире в 1997 году являются пиратскими, что по оценкам принесло убыток в 11.4 миллиардов долларов. Самые большие убытки понесли Соединенные Штаты - около 2.8 миллиардов долларов, тогда как в Китае по оценкам доля нелицензионного программного обеспечения составляет 96%.

Согласно этим результатам, U.S. Trade Representative издали список "Special 301", которые концентрирует внимание на странах допускающих пиратство на своих территориях. Особо сложно с индустрией программного обеспечения дела обстоят в Китае, Тайване, Парагвае и Болгарии. Факт, что только International Digital Software Association (IDSA) теряет 3.2 миллиардов на продаже программного обеспечения.

С приходом технологий CD-R и их стремительного удешевления пиратство стало еще более распространенным легким занятием, тогда как индустрия развивается. Убытки становятся колоссальными.

Взглянем на проблему несанкционированного копирования с другой стороны. Так как CD не обладают 100%-ной надежностью, многие люди хотели сделать бэкап своих игр. Используя бэкап для того чтобы играть в игры, МЫ сохраняли оригинал. Если у вас есть дети, то бэкап вам просто необходим. Но из-за различных защитных уловок становится все сложнее и сложнее сделать просто рабочую резервную копию.

Обратите внимание, что во многих странах РАЗРЕШАЕТСЯ делать копию CD, который вам принадлежит. Некоторые компании не хотят позволять делать копии, оговаривая это тем, что испорченный оригинал они могут заменить, но во многих случаях цена замены выше, чем цена самой игры !

Эта работа посвящена известным способам защиты от несанкционированного копирования коммерческого программного обеспечения, распространяемого преимущественно посредством оптических носителей, описанию принципов работы этих технологий, способам определения конкретной защиты. А также как можно обойти такую защиту и все-таки сделать "резервную копию", описанию полезных программ.

Перейдем непосредственно к рассмотрению наиболее популярных коммерческих технологий защиты от несанкционированного копирования CD.

CD-Cops.

Эта система защиты была создана датской компанией Link Data Security, основанной 1982. В 1984 году появилась первая версия Cop's Copylock под DOS. В дальнейшем они выпустили полную линейку продуктов под DOS, Windows и NT. Защищенные приложения можно распространять на дискетах, CD, DVD. В любом случае приложение привязано к исходной дискете, CD, DVD, то есть необходимо наличие оригинального носителя в устройстве для того, чтобы запустить уже инсталлированную программу. Любые копии CD на CD-R отвергаются, причем даже изготовленные на заводском оборудовании штампованные диски также не позволяют запускать программу. Даже копии, изготовленные при помощи CloneCD отказываются работать.

При инсталляции купленного приложения нужно чтобы пользователь ввел 8-значный код, который входит в комплект с продуктом.

Link Data Security распространяет свои защитные программные продукты по цене 2000$ за однопользовательскую версию CD-Cops и 3500$ за сетевую версию CD-Cops NET.

Обнаружить присутствие защиты CD-Cops иногда бывает очень просто. Как правило в инсталляционном дистрибутиве приложения содержат файлы с расширениями .GZ_ и .W_X, иногда можно найти файл CDCOPS.DLL. Бывает также, что заголовок окна запущенного приложения содержит CD и Cops.

Теперь несколько слов о принципах работы этой защиты. Как говорится, «все гениальное - просто». CD-Cops не использует электронный код в качестве «отпечатков пальцев». Проверяется только физический угол между первым и последним доступным логическим сектором на диске. Как показывает опыт эта характеристика не сохраняется постоянной при изготовлении мастер-диска или CD-R копии, однако сохраняется при штамповании копий с мастер-диска, для которого эта характеристика известна. При этом производителю не нужно какое-либо специальное оборудование, 8-значный код содержит информацию об угле, а проверка подлинности лишь сверяет его с измеренным для данного диска.

Как уже было сказано, CloneCD не справляется с этим способом защиты, однако существуют другие утилиты, такие как CD-Cops Decrypter, позволяющие справиться с CD-Cops.

Alcatraz

Alcatraz - новая разработка компании KDG. По сути дела защита представляет что-то среднее между SecuROM и SafeDisc. Используется система так называемых "водяных знаков". Также известно, что технология защиты достаточно гибкая и защищаемое программное обеспечение изменяется на стадии изготовления стеклянной мастер-копии.

Упоминается также о Level 3b Protection, что может выражаться в совершенно различных симптомах, от предупредительного сообщения, до падения системы и переформатирования жесткого диска.

Пока еще примеров применения данной защиты нет, также и неизвестно как с ней бороться. Должно быть это "крепкий орешек".

Dummy Files / CD Lock

Смысл этой защиты состоит в том, что создаются большие файлы, указывающие на различные части файловой системы, уже занятые другими файлами. При попытке скопировать CD на жесткий диск или CD-R, получается, что суммарный объем явно больше, чем может уместиться на обычный CD-ROM. Зачастую получается больше 2 Gb.

Вместе с защитой методом создания некорректного TOC, это может случить примитивной защитой от несанкционированного копирования.

Отличить эту защиту от других можно, найдя больший "dummy" файлы, причем как правило в корневой директории CD и как правило с расширением .AFP.

Обойти эту защиту проще простого. Если копируемый CD меньше 659 Mb, просто сделайте копию (DAO/TAO), которая воспроизведет и dummy files на диске. Если этот CD больше 659 Mb - возьмите болванку побольше.

LaserLock

MLS LaserLock International специализируется на исследовании и разработках в области защиты программного обеспечения. Компания была основана в 1989 году в Греции и была первой компанией, которая выпустила на рынок законченную систему защиты CD от копирования. Именно этому и обязана достаточно высокая популярность этого способа защиты.

Защита обеспечивается путем изысканного шифрования программы; физической подписи на CD, вносимой на стадии изготовления уникальной мастер-копии; внедрения в двоичный код приложения системы защиты от взлома метода отладки. Рассмотрим схему защиты несколько подробнее:

Шаг 1. Заполняем формы "Application Description" форма A1 и "LaserLock Order" форма 2 и отправляем их вместе с мастер-копией защищаемого приложения на CD-R ближайшему авторизованному дилеру LaserLock.

Шаг 2. Согласно форме "Application Description", MLS подготовит определенный набор файлов и библиотек, которые будут использованы при встраивании защиты в ваше приложение.

Шаг 3. Высококвалифицированные программисты встроят защиту LaserLock в код вашего приложения. Получается новая мастер-копия на CD-R, содержащая все ту же инсталляцию вашего приложения, но уже с защитой LaserLock.

Шаг 4. Вам высылают 5 штампованных копий вашего приложения с защитой. Если вы одобряете работу, то вам делают матрицу, с которой можно штамповать диски на любом подходящем заводе.

MLS предоставляет некоторые требования к приложению: желательно, чтобы запускаемые файлы были в 32-битном формате; если инсталляция происходит из сжатого архива, должен быть доступ к несжатым исполняемым файлам; защита занимает от 12 до 20 Mb места, поэтому необходимо, чтобы на золотой мастер-копии было достаточно свободного места.

Обнаружить эту защиту несложно. В корне защищенного CD находится скрытая директория LaserLock, в которой находятся файлы Laserlock.in, Laserlock.o10, Laserlock.o11. Эта директория заполняет нечитаемый сектор, который визуально можно распознать на рабочей поверхности CD в виде тонкого колечка.

Это один из тех примеров, когда затраты на защиту практически себя не окупают. Программные продукты, защищенные LaserLock без труда копируются при помощи CloneCD. Существуют также патчи LL32ICA Generic LaserLock Patch и LaserLock Import Fixer, которые снимают большинство версий защиты. Копию можно также сделать, использовав любую утилиту, поддерживающую чтение в режиме RAW, например DDump или BlindRead. В крайнем случае содержимое нечитаемых файлов можно перенести в HexEditor.

ProtectCD

Эта технология защиты никак не изменяет данные на CD, но записывает различные служебные данные в различных частях файловой системы CD, доступные только для самой защитной системы.

Симптомы:

Программы защищенные этим методом ходят на любой машине, правда только если в CD-ROMe находится ключевой диск. Нет необходимости вводить какие-либо серийные номера и ключи. С диском можно делать все что вздумается, кроме копирования. Смысл защиты заключается в том, что на защищенном диске присутствует дополнительная область, и такие диски могут производиться только на авторизованных заводах.

Технология ProtectCD доступна в виде двух реализаций, которые различаются по простоте применения к программному продукту, и, соответственно, по уровню защиты. Уровень II заключается в том, что вы получаете от VOB набор библиотек, которые необходимо привинтить к исходному коду программы, тогда как уровень I реализован в виде программы, изменяющей двоичный код вашего приложения автоматически. Вся простота применения уровня I компенсируется, тем, что защита проверяет подлинность только единожды при запуске защищенного приложения и отсутствует защита от взлома методами отладки.

Для справки: данный продукт от VOB стоит 1500$ на один продукт, плюс что-то там еще, за каждый изготовленный на авторизованном заводе диск.

Обнаружить присутствие защиты достаточно просто. Откройте главный исполняемый файл приложения при помощи HexEditor и поищите ASCII-текст VOB. Это сочетание должно встречаться несколько раз.

CloneCD и BlindRead прекрасно справляются с ProtectCD, если CD-Reader поддерживает чтение в режиме RAW (MMC DAO RAW), а пишущий привод поддерживает Sub-Channel запись.

SafeDisc

Технология защиты довольно стандартна: цифровая подпись, которая не переносится при копировании; шифрование запускаемого файла, защита от попыток взлома отладкой. SafeDisc работает со стандартными процедурами премастеринга, мастеринга и штампования. В процессе премастеринга содержимое шифруется с использованием достаточно простого ПО. Затем зашифрованная версия записывается на "золото". На стадии изготовления стеклянной мастер-копии цифровая подпись вносится при помощи оборудования, контролируемого Doug Carson Associates(DCA) Mastering Interface Software (MIS). После производится репликация нужного количества копии и соответствующие тесты.

На всех защищенных CD можно найти следующие файлы:

00000001.TMP
CLCD16.DLL
CLCD32.DLL
CLOKSPL.EXE
DPLAYERX.DLL

Также присутствуют файлы GAME.EXE и GAME.ICD, где .ICD - настоящий исполняемый файл приложения (зашифрованный), а .EXE осуществляет загрузку защитного аппарата SafeDisc.

Возможные пути снятия защиты:

1.Если ваш как читающий, так и пишущий приводы поддерживают режим RAW (MMC DAO RAW) - можно делать копию 1:1. В этом случае можно использовать BlindRead или DDump.

2.Сделав копию 1:1 используйте Generic SafeDisc Patch or DAEMON Tools, чтобы снять защиту.

3. unSafeDisc и DumPlayerx умеют вытягивать настоящий .EXE файл из зашифрованного .ICD, Вытянутый файл можно потом сохранить как .EXE, а потом делать сколько угодно копий.

SecuROM

Технология защиты от копирования Securom создана Sony и является достаточно распространенной. Эта система подтверждает подлинность CD оригинальным методом. "Отпечатки пальцев" подлинного CD вносятся при специальном процессе DADC на стеклянную мастер-копию и являются уникальными для каждого продукта. В сочетании с технологией шифрования приложения это делает защиту достаточно эффективной от любых видов нелицензионного распространения ПО. Система не требует, чтобы пользователь вводил какие либо цифровые ключи. "Отпечатки пальцев" вносятся в процессе изготовления стеклянного мастер-диска. Каждая новая мастер-копия характеризуется уникальным номером. Способы обезвреживания защиты существуют, однако последние версии SecuROM умеют определять, запускается программа с CD-ROM или с CD-R, и в случае запуска с CD-R срабатывает защита (известный случай - V-Rally 2).

Установка защиты на приложение производится на предприятии Sony DADC. Никаких изменений в исходном коде программы производить не нужно. Нужно только указать главный запускаемый файл приложения, на которое необходимо установить защиту.

Во многих случаях в инсталляционном дистрибутиве приложения можно найти файлы CMS16.DLL, CMS_95.DLL и CMS_NT.DLL, но это не обязательно. На внутреннем кольце также очень часто можно найти небольшой логотип В бинарном коде приложения также можно найти сочетание символов CMS.

Можно попробовать копировать диск при помощи CloneCD. Также существуют резидентные патчи DAEMON Tools и Generic SecuROM Patches для многих версий защиты .

Некорректный TOC (Table of Contents)

Название этой методики защиты говорит само за себя. Как правило обнаружить ее можно, если посмотреть на треки копируемого диска. Обычно это выглядит как то, что на CD содержится второй трек с данными, обычно после нескольких аудио-трэков. Во многих программах записи CD-R есть опция типа Ignore Illegal TOC, которая позволяет без труда записать такой диск.

Переполнение (oversize/overburn) CD

Многие штампованные диски имеют объем больше 659 Mb, поэтому большинство CD-Recorder'ов не захотят записывать их на 74-х минутную болванку. С появление 80-ти минутных болванок эта защита стала практически неактуальной. Если переполнение диска производится намеренно, то в избыточной части файловой системы как правило ничего полезного не записано (фактически записана пустота). В принципе переполнять CD-R диски умеют многие современные CD-Recorder'ы, если использовать соответствующее программное обеспечение для записи, например, Nero, CDRWIN, CD Wizard или DiskJuggler.

Физические дефекты

Это достаточно интересная проблема, так как только несколько моделей CD-ROMов способны копировать CD с физическими дефектами (как правило современные модели Teac). Такое копирование может занять много времени, порядка нескольких часов. Например, на диске #1 Settlers 3 во внешней трети читаемой поверхности можно заметить выделяющееся кольцо ок. 1 мм толщиной. Как раз тот случай . На крайний случай, чтобы скопировать нужные файлы, попробуйте использовать BlindRead, BlindWrite или DiscDump.

DiscGuard

Эта технология защиты создана TTR Technologies Inc, основанной в 1994 году. DiscGuard - технология защиты от несанкционированного копирования с оптических носителей. Ее работа основана на внесении цифровой подписи на стеклянный мастер-диск в процессе его изготовления в заводских условиях, используя специальную усовершенствованную мастер-машину, или на CD-R при помощи DG-Author(TM). В двух словах технология затрагивает целевой продукт следующим образом:

- Главные запускаемые файлы приложения, на защищенном DiscGuard CD-ROM зашифрованы.
- Специальная цифровая подпись записана на CD-ROM и отображена в дешифрующем ключе приложения. Цифровая подпись не воспроизводится при производстве как методами штамповки, так и копированием на CD-R.

Когда используется подлинный диск, подпись присутствует, осуществляется дешифровка приложения и оно запускается. Пользователь даже и не подозревает, что программный продукт защищен. При использовании копии, дешифровка не происходит, следовательно приложение не запускается. Вместо этого появляется сообщение, ссылка на коммерческий сайт производителя или распространителя ПО, иногда запускается ограниченная демо-версия или мультимедиа-презентация. Это дает возможность превращать нелегальную копию в инструмент маркетинга и рекламный продукт.

Создание защиты DiscGuard.

1. Защита:

Издатель ПО защищает продукт используя приложение TTR DG-Protector. DG-Protector шифрует исполняемые файлы (.EXE) и добавляет возможность обнаруживать правильную подпись DiscGuard. Для подтверждения работоспособности защиты можно инсталлировать приложение и испытать его с тестовым ключом.

После тестирования издатель записывает "Client Master" CD-R, содержащий полный программный пакет, включающий защищенные файлы, и посылает его на авторизованный завод DiscGuard с необходимой документацией.

2. Премастеринг:

Изготовление премастер-копии DiscGuard из Client Master, используя программное обеспечение TTR's DG-Works на упомянутом выше заводе. Премастер-копия содержит дополнительную информацию, необходимой для создания цифровой подписи, которая будет использоваться машиной изготовления мастер-копии.

3. Мастеринг:

TTR-авторизованном производстве из премастер-копии изготовляется стеклянная мастер-копия, содержащая цифровую подпись DiscGuard. Теперь дело стоит только за процессом тиражирования.

Обнаружить эту защиту очень просто - в инсталляционной директории присутствуют файлы IOSLINK.VXD и IOSLINK.SYS.

Что касается надежности защиты этим способом, то можно с уверенностью сказать, что сложность производства себя оправдывает. CloneCD бессилен перед DiscGuard, поэтому ничего не остается, как копаться в двоичном коде.

Известные случаи применения этой защиты: Protected Collin McRae Rally.

Выводы:

Развитие высоких технологий вызвало появление нового типа преступлений – компьютерного пиратства. С приходом технологий CD-R пиратство стало еще более распространенным и легким занятием.

Современные технологии защиты от копирования не могут гарантировать сохранность интеллектуальной собственности. Многие из них совершенно отстали от уровня развития пишущей техники и не оправдывают себя.

По-видимому, вопрос защиты интеллектуальной собственности никогда не утратит свою актуальность, и дальнейшее развитие индустрии потребует введения более надежных и удобных средств защиты.

При подготовке доклада использовались материалы сайтов:

Общая информация:
http://www.flexdata.ru/
http://www.ixbt.com/
http://www.compulenta.ru/

Сайты производителей:
http://www.macrovision.com/solutions/software/cdrom/
http://www.kochdigi.com/en/1/product_d_6.html
http://www.linkdata.com/index.htm#cdcops
http://www.ttrtech.com/tech.htm
http://www.laserlock.com