**Министерство образования и науки Украины**

**НТУУ «КПИ им. И.Сикорского»**

**Кафедра АПЭПС**

Отчет к лабораторной работе №4

Дисциплина: «*Безопасность программ и данных*»

Тема: *« Методы защиты исходных кодов .Net-приложений»*

12 вариант

Выполнил: студент 4 курса  
 ТЭФ, ТИ-31  
 Николаев В.В.

Проверил: Тарнавский Ю.А.

Киев-2016

**Цель работы:** Ознакомиться с возможностями обфускации и использования упаковщиков для защиты кода от дизассемблирования.

**Инструменты и дополнительные файлы:** онлайн обфускатор Appfuskator, дизассемблер ILSpy, архиватор WinRar, учебное приложение HackOfCode.exe.

**Выполнение работы**

***1.Функциональные особенности Appfuskator***

Ниже перечислены методы защиты, а также алгоритмы интеллектуального анализа кода и ресурсов, реализованные в ***Appfuskator***:

**Renaming**

Переименование классов и их членов, с полной поддержкой Generics, наследования, перегрузки виртуальных методов, анализа стандартных атрибутов обфускации.

**Assembly Merging**

Объединение сборок — объединение кода из нескольких исходных защищаемых сборок в одну.

**Decomposition**

Декомпозиция структуры классов в процедурное представление — уникальная разработка нашего продукта, базирующаяся на идее перевода программы из объектно-ориентированной формы (простой для реверс-инжиниринга) к процедурному стилю, с максимальным уничтожением всей доступной информации хранимой в метаданных (но с сохранением полной работоспособности сборщика мусора).

**Control Flow Obfuscation**

Запутывание потока управления — cокрытие кода алгоритмов программы, путем создания запутанной разветвленной логики, сложной для анализа (реальные и ложные ветвления, switch переходы и другие методы). Инными словами, так называемый spaghetti code. Поведение самой программы при этом не изменяется.

**External Method Call Hiding**

Скрытие вызова внешних методов — подмена явного вызова методов из внешних сборок (в том числе обращений к Common Language Runtime), на неявное обращение по неуправляемому указателю, извлеченному из метаданных на основе зашифрованного идентификатора.

**String Encryption**

Шифрование строк на основе собственного алгоритма. Использует динамические переменные и шифрованные блоки данных с целью максимального усложнения потенциальной автоматической де-обфускации.

**WPF Obfuscation**

Автоматическое определение и корректная обфускация типов, методов и полей, к которым имеются обращения из Windows Presentation Foundation. Работает на базе декомпиляции и дальнейшей повторной сборки BAML ресурсов, за счет чего достигается переименовывание максимально возможного количества данных.

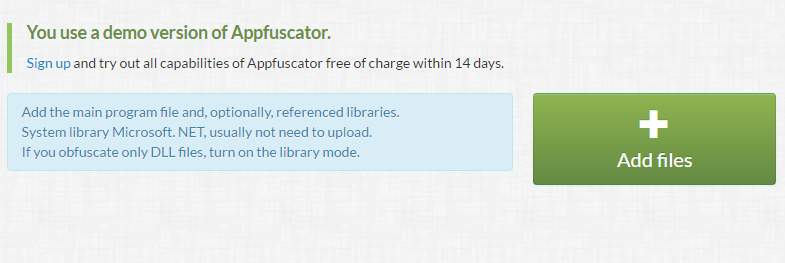
**Reflection Analyzing**

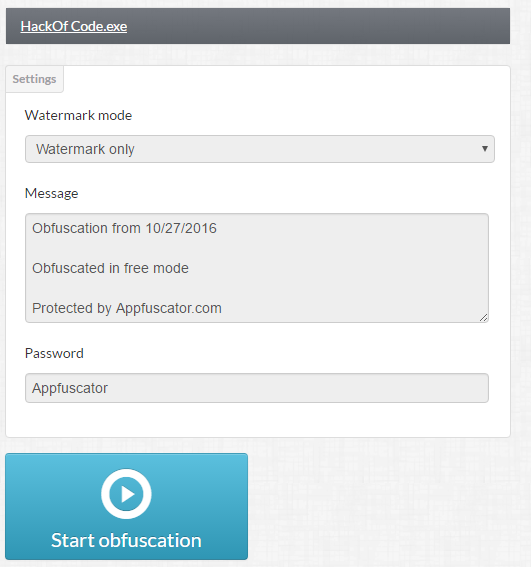
Анализ обращений к механизму отражения — набор алгоритмов, отслеживающих обращение к Reflection методам (как к методам явного обращения по имени, так и к перечислениям членов класса). Автоматически отслеживает связи и корректирует имена в исходном коде.

***2. Как выполнить обфускацию файла с помощью Appfuskator***

Переходим на сайт [разработчика](http://appfuscator.com/).

Находим интерфейс бесплатного создания защищенных сборок.



Выбираем сборку на ПК

Запускаем обфускацию, после чего можем получить новую сборку.

***3. Какие виды обфускации доступны при использовании онлайн версии Appfuskator?***

При использовании ***Appfuskator*** в онлайн режиме доступен только режим ***Watermark.***

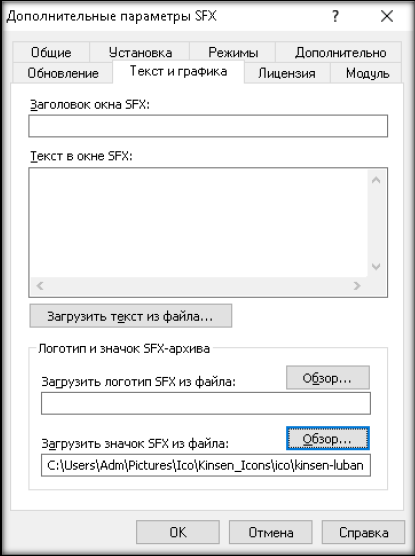
***4. Какие возможности по созданию SFX-архивов предоставляет WinRar?***

[SFX-модули](http://winrar.pp.ua/html/HELPGUISFX.htm) WinRAR с графическим интерфейсом (GUI) поддерживают несложные команды для создания инсталляционных пакетов. Эти команды должны находиться в [комментарии](http://winrar.pp.ua/html/HELPArcComment.htm) SFX-архива. Ниже приведён список команд. Щёлкните по названию команды, чтобы ознакомиться с её подробным описанием.

|  |  |
| --- | --- |
| [Delete](http://winrar.pp.ua/html/HELPSFXDelete.htm) | Удалить файл перед извлечением |
| [License](http://winrar.pp.ua/html/HELPSFXLicense.htm) | Показать экран с лицензионным соглашением |
| [Overwrite](http://winrar.pp.ua/html/HELPSFXOverwrite.htm) | Выбор режима перезаписи файлов |
| [Path](http://winrar.pp.ua/html/HELPSFXPath.htm) | Установить предлагаемый по умолчанию путь для распаковки |
| [Presetup](http://winrar.pp.ua/html/HELPSFXPresetup.htm) | Выполнить указанную программу до начала распаковки |
| [SavePath](http://winrar.pp.ua/html/HELPSFXSavePath.htm) | Сохранить путь назначения |
| [Setup](http://winrar.pp.ua/html/HELPSFXSetup.htm) | Выполнить указанную программу после успешной распаковки |
| [Shortcut](http://winrar.pp.ua/html/HELPSFXShortcut.htm) | Создать ярлык для распакованного файла |
| [Silent](http://winrar.pp.ua/html/HELPSFXSilent.htm) | Не показывать начальный диалог |
| [TempMode](http://winrar.pp.ua/html/HELPSFXTempMode.htm) | Распаковать архив во временную папку |
| [Text](http://winrar.pp.ua/html/HELPSFXText.htm) | Добавить текст в диалоговое окно SFX-архива |
| [Title](http://winrar.pp.ua/html/HELPSFXTitle.htm) | Указать заголовок диалогового окна SFX-архива |
| [Update](http://winrar.pp.ua/html/HELPSFXUpdate.htm) | Выбор режима обновления файлов |

***5. Как изменить стандартный значок SFX-архива, созданного в WinRar?***

При создании архива, используя графический интерфейс, указываем пусть к файлу в следующем интерфейсе



При создании архива используя командую строку нужно указать параметр **–iicon “%image\_path%”**, где **image\_path** – абсолютный путь к иконке. Пример команды :

***winrar a -r -m5 -ma5 -iiconc:\%icoFile%.ico -z"xfile.conf" -p -sfx D:\%nameFile% "HackOf Code\_obf.Patched.exe"***

***6. Как создать в WinRar-архив в режиме командной строки? Какие ключи при этом могут использоваться?***

Для создания архива, используя командную строку, необходимо добавить папку с установленным WinRAR в переменную **Path** среды Windows. После, используя командную строку можно вводить команду для архивирования файлов используя разные настройки.

**Примеры:**

а) Добавить все файлы \*.hlp из текущей папки в архив help.rar :

**WinRAR a help \*.hlp**

б) Заархивировать все файлы из текущей и вложенных папок в самораспаковывающийся непрерывный архив, разделённый на тома save.part1.exe, save.part2.rar, save.part3.rar, … размером по 362000 байт, и добавить к каждому тому информацию для восстановления:

**WinRAR a -r -v362 -s -sfx -rr save**

Так как имена обрабатываемых файлов не указаны, подразумеваются все файлы (\*.\*).

в) Как особое исключение, если в качестве аргумента указано имя папки, и это имя не содержит файловых масок и завершающих символов обратной косой черты (\), то в архив будет добавлено всё содержимое указанной папки и её вложенных папок, даже если не указан [ключ -r](http://winrar.pp.ua/html/HELPSwR.htm). Следующая команда добавит все файлы из папкиBitmaps и вложенных в неё папок в RAR-архив Pictures:

**WinRAR a -r Pictures.rar Bitmaps**

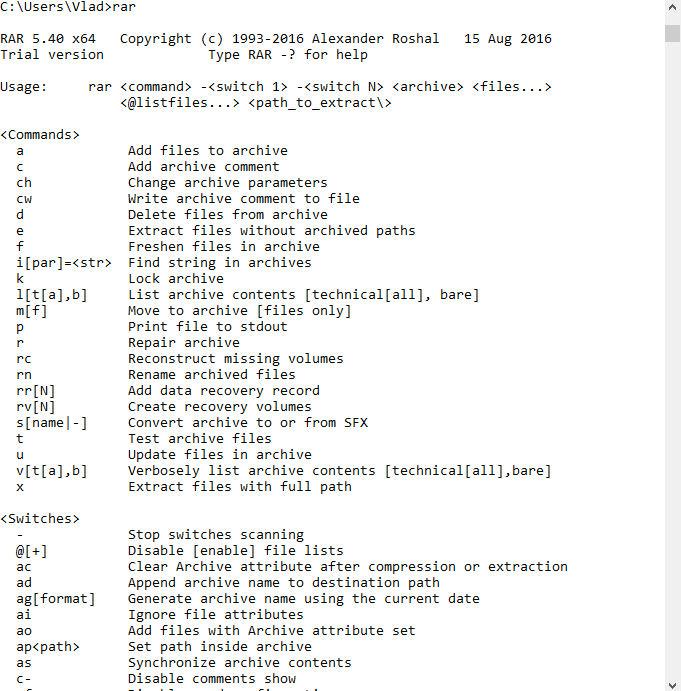
г) Если в имени папки содержатся файловые маски или завершающие символы обратной косой черты, то применяются обычные правила, и чтобы включить в обработку вложенные папки, необходимо указать [ключ -r](http://winrar.pp.ua/html/HELPSwR.htm).

Следующая команда добавит все файлы из папки Bitmaps, но не из её вложенных папок, так как ключ -r не указан:

WinRAR a Pictures.rar Bitmaps\\*

Список ключей можно просмотреть введя команду rar/winrar в консоли без параметров

**Пример:**



***7. Какими командами Windows можно воспользоваться для организации диалога с пользователем в режиме командной строки?***

Для организации простейшего диалога с пользователем, используя командную строку, можно применять следующий **batch** код

***@echo off***

***set /p id="Enter ID: "***

**Заключение:**

Я научился использовать программу[**Appfuscator**](http://appfuscator.com/)в режиме онлайн, и онлайн режиме. Изучил методы защиты кода, которые он предоставляет. Используя программу **IlSpy,** изучил изменения кода сборки этой программой. Научился создавать защищенные архивы, самовыполняющиеся архивы, используя программу **WinRAR**. Изучил базовые команды для создания архивов, используя командную строку и приложение **rar/winrar.**