

Декомпилируем инсталляторы InnoSetup

📁 HOWTO 🕒 01.10.2014 💬 28 комментариев

В данной статье мы подробно рассмотрим как осуществить полную декомпиляцию программ установки, созданных при помощи популярного средства — InnoSetup. На выходе мы получим всё содержимое архива, а также полный исходный код установщика.

Введение

В качестве примера мы будем осуществлять декомпиляцию нашего проекта [SRC Repair](#), распространяющегося по лицензии GNU GPL v3, программа установки (далее «инсталлятор») которого собрана при помощи InnoSetup.

Загрузка компонентов

Для начала нам потребуется утилита [Inno Setup Unpacker](#) версии 0.40 (поддерживает все версии InnoSetup до 5.5.4 включительно). Загрузить её можно [здесь](#). Распакуйте архив в любой каталог, например, **C:\iunp**.

Также для разбора секции **code**, которая компилируется в бинарный файл, нам потребуется дизассемблер **ROPS**, который можно взять [здесь](#). Распаковать его следует в тот же каталог.

Теперь скачаем SRC Repair последней версии по [прямой ссылке](#).

Краткая справка по декомпилятору

Т.к. утилита InnoSetup Unpacker (далее просто «Unpacker») работает из командной строки, рассмотрим основные ключи:

```
1 | innounp.exe [команды] [параметры] <имя_установщика.exe> [@список_файлов] [маска]
```

В квадратных скобках указываются необязательные параметры. Единственным обязательным является имя файла инсталлятора, который мы будем декомпилировать.

Список допустимых команд утилиты innounp:

- **-v** — вывести список файлов архива (с размерами и датами создания/изменения);
- **-x** — распаковать файлы из архива в текущий каталог (допускается указать параметр -d для указания другого каталога назначения);
- **-e** — распаковать файлы в текущий каталог без соблюдения внутренней структуры каталогов;
- **-t** — запустить проверку целостности архива.

Список допустимых параметров утилиты innounp:

- **-b** — включает неинтерактивный режим. Рекомендуются для использования в скриптах;
- **-q** — подавляет вывод на экран прогресса извлечения файлов из архива;
- **-m** — осуществить глубокую декомпиляцию (при этом будут собраны деинсталляторы, а также извлечён бинарный файл секции code);
- **-pPASS** — задаёт пароль для архива (если он был им защищён);
- **-dDIR** — указывает каталог, в который будет распаковано содержимое архива (допускаются как абсолютные, так и относительные пути);
- **-fFILE** — то же, что и -r, но пароль считывается из указанного текстового файла;
- **-a** — включает обработку дублирующихся файлов внутри архива;
- **-y** — отвечает на все вопросы программы утвердительно (разрешение на перезапись файлов и т.д.).

Декомпиляция примера

1. Откроем командную строку Windows (**Пуск — Выполнить — cmd.exe**).
2. Перейдём в каталог, в который установили Unpacker (**C:\iunp**):

```
1 | cd /D "C:\iunp\"
```

3. Скопируем в этот же каталог установщик, который будем декомпилировать (в нашем случае это SRC Repair).
4. Выполним в консоли команду:

```
1 | innounp.exe -x -m -dout srcrepair_180_final.exe
```

5. В случае успеха в каталоге **C:\iunp\out** мы найдём всё содержимое установщика, а также файл с расширением *.iss, который является полным исходным кодом модуля установки (включая комментарии).
6. Если в скрипте установки были вставки кода, то в каталоге **C:\iunp\out\embedded** будет находиться бинарный файл **CompiledCode.bin**, который содержит его в скомпилированном виде.

Дизассемблирование файла CompiledCode.bin

1. Снова откроем командную строку Windows.
2. Перейдём в каталог, в который распаковали **ROPS (C:\iunp\)**:

```
1 | cd /D "C:\iunp\"
```

3. Выполним в консоли команду:

```
1 | disasm.exe out\embedded\CompiledCode.bin out.asm
```

4. В файле **C:\iunp\out.asm** мы найдём дизассемблированный код.

Заключение

Таким образом, мы получили полное содержимое программы установки, собранной при помощи InnoSetup, включая её полные исходные коды.

28 commentaries to post



HEMULGM

29.04.2015 в 18:54

Хорошая статья. Без лишних слов. Прочитал, понял и в течении двух минут закрепил на практике. Благодарю. (Хотя, кажется мне я поздновато её прочёл.)



АНДРЕЙ

23.01.2019 в 14:30

Скрипты не распаковывает. Они все пустые.



VITALY

25.01.2019 в 19:27

К сожалению, проект уже не развивается и не может распаковывать установочные пакеты, созданные новейшей версией InnoSetup.



SOL

12.08.2019 в 12:10

Распаковывает, только может с кодировкой начудить. Часть строк в UTF-8, часть в win-1251, так что после распаковки и доработки напильником действительно открывается корректно в InnoSetup GUI.



VITALY

12.08.2019 в 15:04

Зависит от того, в какой версии InnoSetup был собран оригинальный установщик: ANSI или Unicode.

Самая актуальная версия InnoSetup 6 поддерживает только юникод.



ЕВГЕНИЙ

20.03.2016 в 00:28

Проканает только на старых версиях инно.

На 5.0+ стандартный крипток и почти все используют сторонние dll по дефолту.



VITALY

21.03.2016 в 03:28

@Евгений

Inno Unpacker прекрасно распаковывает даже установщики, собранные новейшей версией InnoSetup — 5.5.8.



АЛЕКСАНДР

15.07.2016 в 21:07

Хоть и статья 2014 но у меня вопрос как это дело после разбора собрать? У меня после дизассемблирования файла CompiledCode.bin инно не хочет принимать код выкидывает ошибку хоть я не очень понимаю куда его вставлять (вставлял туда и где весь другой код) но установщик был собран на старой версии 4.2.6 а на ней я вообще не понимаю как это дело все собрать так что пытался на 5.5.9. Просто хотел разобрать/собрать но не получилось ☹



VITALY

16.07.2016 в 18:45



@Александр

CompiledCode.bin разбирается в псевдокод, его нельзя скомпилировать заново.



АЛЕКСАНДР

18.07.2016 в 18:25

То есть для обычного пользователя это не реально? ☐ А что нужно сделать с ним что бы скомпилировать заново? Или это делается так что бы посмотреть что и как?



VITALY

24.07.2016 в 18:04

@Александр

Нет, собрать такой дизассемблированный CompiledCode.bin из псевдокода не представляется возможным.



DMITRY

25.10.2016 в 16:26

А не проще открыть инсталлятор через 7-Zip?

т.е. для вас сообщаю что некоторые exe файлы можно открывать через zip архиваторы. (Насчет рара не знаю не пробовал) Через 7-Zip можно и получить исходный код программы НО иногда. Не знаю точно но я находил исходный код установщика внутри него!

А так же можно изменять инфу о приложении по скольку это все хранится (по крайней мере у меня) в отдельных файликах.

И предупреждение. Некоторые разработчики знают о такой функции архиваторов и потому как они на exe файл как на архив ставят пароль. Просто так предупредил об этом.

Ну, может кому то понадобится...



VITALY

25.10.2016 в 17:16

Dmitry :

А не проще открыть инсталлятор через 7-Zip?

Далеко не все форматы установочных пакетов InnoSetup можно открыть в 7-Zip. Можете попробовать например описанный в статье пример с SRC Repair. Открыть его в 7-Zip даже последней версии невозможно.

Dmitry :

т.е. для вас сообщаю что некоторые exe файлы можно открывать через zip архиваторы. (Насчет рара не знаю не пробовал)

Разумеется если это по сути SFX-архивы.

Dmitry :

А так же можно изменять инфу о приложении по скольку это все хранится (по крайней

мере у меня) в отдельных файликах.

Это хранится в ресурсе. Конечно же можно изменять при помощи редактора ресурсов.

Dmitry :

И предупреждение. Некоторые разработчики знают о такой функции архиваторов и потому как они на ехе файл как на архив ставят пароль. Просто так предупредил об этом.

Если на сам контейнер установлен пароль, то InnoSetup будет запрашивать его перед установкой, т.к. содержимое внутри зашифровано стойким алгоритмом AES-128. Описанная в статье утилита декомпилятор отлично умеет распаковывать и зашифрованные установочные пакеты если передать ей пароль в качестве параметра.



АДМИНЫЧ

01.07.2017 в 17:27

А где взять disasm.exe?



VITALY

01.07.2017 в 19:48

Здесь. В статье об этом сказано.



АЛЬБЕРТ

03.09.2017 в 06:47

Не удастся найти указанный файл



VITALY

03.09.2017 в 15:39

Какой файл? Если строго следовать инструкции, всё будет работать.



ВЛАД

01.02.2018 в 13:18

Version detected: 5500

Critical error: The setup files are corrupted. Please obtain a new copy of the program.

Вот что пишет при попытке декомпилировать.



VITALY

02.02.2018 в 00:01

Вы пытаетесь декомпилировать либо повреждённый установщик, либо зашифрованный, либо

собранный более свежей версией Inno Setup.



AQEL

01.06.2018 в 09:00

Есть наработки по поиску пароля (на архивы) в файле CompiledCode



VITALY

02.06.2018 в 02:43

Содержимое установочных пакетов InnoSetup **шифруется ARCFOUR (RC4)**, поэтому пароль нигде не хранится и восстановить его возможно лишь полным перебором:

The password itself is not stored as clear text; it's stored as a 160-bit SHA-1 hash, salted with a 64-bit random number.



ZENXA

18.06.2018 в 20:46

Жалко, но похоже забросили проект, версия 0.46, удалось вскрыть IS 5.5.7, хотя на сайте вроде как и указано что должен распаковывать версию IS 5.5.9, но анпакер ее не берет, сообщение что то типа этого:

Version detected: 5500

Critical error: The setup files are corrupted. Please obtain a new copy of the program.

Ну а про версию 5.5.9(а) вообще можно забыть, если конечно люди делавшие анпакер не обновят свою прогу.



SLAVIK

19.06.2018 в 14:05

<https://constexpr.org/innoextract/>

Нашел то что работает с новыми версиями, и поддерживается.



VITALY

19.06.2018 в 23:44

Спасибо. Утилита [innoextract](#) ещё и кросс-платформенная.



KT

20.06.2018 в 23:35

У InnoExtract есть серьезный недостаток — она не умеет реконструировать ISS скрипты из

готовых инсталляторов.



VITALY

21.06.2018 в 00:18

В баг-трекере проекта уже есть [соответствующий тикет](#).



SERJ

14.10.2020 в 18:11

Очень нужны исходники .iss от «System software for Windows», а именно «Installer.exe», сделанный с помощью Inno Setup. Делаю по инструкции, но выдаёт ошибку:

Version detected: 5500

Critical error: The setup files are corrupted. Please obtain a new copy of the program.



VITALY

19.10.2020 в 19:12

Возможно, инсталлятор был создан в более новой версии InnoSetup, чем поддерживает данная утилита.

Обсуждение закрыто.

[◀ Удаляем повреждённые пакеты в Fedora](#)

[Добавляем поддержку Skype в Pidgin >](#)



РАЗДЕЛЫ САЙТА

 [HOWTO](#) (87)

 [Новости](#) (8)

 [Программирование](#) (7)





 [Разное](#) (3)

 [Разработка](#) (18)

 [Рецензии](#) (3)

СВЕЖЕЕ НА САЙТЕ

 [Настраиваем поддержку UEFI Secure Boot для драйверов NVIDIA](#)

-  [Используем TPM для хранения SSH-ключей](#)
-  [Работаем с GPG подписями и шифрованием в C#](#)
-  [Обходим проверку на наличие прав суперпользователя](#)
-  [Управляем профилями производительности Linux](#)