Python-скрипты для анализа PE-файлов

Release 0.0.1

Дроботун Евгений

Jul 08, 2021

Contents

Руководство по использованию пакета pefile_scripts.

CHAPTER 1

Общие сведения о пакете

Пакет включает в себя четыре модуля:

- get_time_info - содержит функции для получения времени компиляции PE-файла.
- get_section_info - содержит функции для получении информации о секциях PE-файла. Позволяет получать информацию о количестве секций в PE-файле, их названиях, значения поля Characteristics, значения MD5-хэша и энтропии для каждой секции.
- get_import_info - содержит функции для получения информации о таблице импорта PE-файла. Позволяет получать информацию о количестве импортируемых dll-библиотек, значение imphash, а также список импортируемых api-функций для каждой dll-библиотеки.
- get_export_info - содержит функции для получения информации о таблице экспорта PE-файла. Позволяет получать информацию о количестве экспортируемых функций, имена экспортируемых функций (при их наличии), а также значения номеров (ординалов) и значения RVA-адресов для всех экспортируемых функций.

1.1 Инсталляция пакета

```
pip install pefile_scripts
```

1.2 Примеры использования

1.2.1 Командная строка

```
python -m pefile_scripts [-ct <путь к файлу>] [-cdt <путь к файлу>] [-crt <путь к файлу>] [-sn <путь к
↪файлу>] [-si <путь к файлу>]
                    [-dn <путь к файлу>] [-ih <путь к файлу>] [-ii <путь к файлу>] [-ean <путь к файлу>] [-
↪edn <путь к файлу>]
                    [-ei <путь к файлу>] [-v] [-h]
```

- -ct, –compilation-time - Время компиляции PE-файла из стандартного поля TimeDateStamp
- -cdt, –debug-compilation-time - Время компиляции PE-файла из секции DIRECTORY_ENTRY_DEBUG
- -crt, –delphi-compilation-time - Время компиляции PE-файла из секции RESOURCE_ENTRY_DEBUG
- -sn, –section-num - Число секций в PE-файле
- -si, –section-info - Информация о секциях PE-файла
- -dn, –dll-num - Число импортируемых dll-библиотек
- -ih, –imphash - Значение imphash таблицы импорта PE-файла
- -ii, –import-info - Информация о таблице импорта PE-файла
- -ean, –export-api-num - Число экспортируемых функций
- -edn, –export-dll-name - Название библиотеки
- -ei, –export-info - Информация о таблице экспорта PE-файла
- -v, –version - Выводит информацию о версии программы
- -h, –help - Выводит справку по программе

1.2.2 Python программы

Модуль get_time_info

get_compile_time()

```
import pefile_scripts

try:
    print('Время компиляции файла:', pefile_scripts.get_compile_time('c:/test_file.exe'))
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

get_debug_compile_time()

```
import pefile_scripts

try:
    print('Время компиляции файла:', pefile_scripts.get_debug_compile_time('c:/test_file.exe'))
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

get_delphi_compile_time()

```
import pefile_scripts

try:
    print('Время компиляции файла:', pefile_scripts.get_delphi_compile_time('c:/test_file.exe'))
```

(continues on next page)

(continued from previous page)

```
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

Модуль get_section_info

get_section_num()

```
import pefile_scripts

try:
    print('Число секций в файле:', pefile_scripts.get_section_num('c:/test_file.exe'))
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

get_section_info()

```
import pefile_scripts

try:
    for section_entry in pefile_scripts.get_section_info('e:/c:/test_file.exe'):
        print(section_entry['name'])
        print('\tCharacteristics: ', section_entry['characteristics'])
        print('\tMD5-хэш секции: ', section_entry['MD5hash'])
        print('\tЭнтропия секции: ', section_entry['entropy'])
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

Модуль get_import_info

get_import_num()

```
import pefile_scripts

try:
    print('Число dll-библиотек в файле:', pefile_scripts.get_dll_num('c:/test_file.exe'))
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

get_imphash()

```
import pefile_scripts

try:
    print('Значение imphash:', pefile_scripts.get_imphash('c:/test_file.exe'))
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

get_import_num()

```
import pefile_scripts

try:
    for import_entry in pefile_scripts.get_import_info('e:/hashcalc.exe'):
        print('Из', import_entry['dll'], 'импортируются:')
        for api_entry in import_entry['api']:
            print('\t', api_entry)
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

Модуль get_export_info

get_export_api_num()

```
import pefile_scripts

try:
    print('Число экспортируемых функций:', pefile_scripts.get_export_api_num('c:/test_file.exe'))
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

get_export_dll_name()

```
import pefile_scripts

try:
    print('Имя dll-библиотеки:', pefile_scripts.get_export_dll_name('c:/test_file.exe'))
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

get_export_info()

```
import pefile_scripts

try:
    for export_entry in pefile_scripts.get_export_info('c:/test_file.dll'):
        print('Имя экспортируемой функции:', export_entry['api'])
        print('\t Номер (ординал):', export_entry['ordinal'])
        print('\t RVA-адрес:', export_entry['rva'])
except pefile_scripts.PEfileScriptsError as err:
    print(err)
```

1.3 Сведения о лицензии

1.4 Исходный код

https://github.com/drobotun/pefile_scripts

1.5 История версий

0.0.1 (22.09.2020)

Базовая версия пакета

CHAPTER 2

Модуль get_time_info

2.1 Функция get_compile_time

Возвращает значение времени компиляции из стандартного поля TimeDateStamp заголовка PE-файла.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Строка в формате {день}-{месяц}-{год} {часы}:{минуты}:{секунды}.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.

2.2 Функция get_debug_compile_time

Возвращает значение времени компиляции из поля TimeDateStamp секции DIRECTORY_ENTRY_DEBUG PE-файла.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Строка в формате {день}-{месяц}-{год} {часы}:{минуты}:{секунды}.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Отсутствует секция DIRECTORY_ENTRY_DEBUG'): В случае, когда в проверяемом файле отсутствует секция DIRECTORY_ENTRY_DEBUG.

2.3 Функция get_delphi_compile_time

Возвращает значение времени компиляции из поля TimeDateStamp секции DIRECTORY_ENTRY_RESOURCE PE-файла. Может применяться для определения даты и времени компиляции PE-файлов, скомпилированных компилятором Delphi (для PE-файлов, скомпилированных компилятором Delphi, стандартное поле TimeDateStamp всегда содержит 0 часов 0 минут 19 июня 1992 года).

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Строка в формате {день}-{месяц}-{год} {часы}:{минуты}:{секунды}.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Отсутствует секция DIRECTORY_ENTRY_RESOURCE'): В случае, когда в проверяемом файле отсутствует секция DIRECTORY_ENTRY_DEBUG.

CHAPTER 3

Модуль get_section_info

3.1 Функция get_section_num

Возвращает число секций в PE-файле.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Число секций в PE-файле.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.

3.2 Функция get_section_info

Возвращает информацию о секциях в PE-файле.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Информация о секциях PE-файла в виде списка объектов типа dict с элементами:

- name - имя секции;
- characteristics - значение поля 'Characteristics';
- MD5hash - значение md5-хэша от секции;
- entropy - значение энтропии секции.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.

CHAPTER 4

Модуль get_import_info

4.1 Функция get_dll_num

Возвращает число импортируемых PE-файлом dll-библиотек.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Число импортируемых PE-файлом dll-библиотек.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Таблица импорта отсутствует'): В случае отсутствия в PE-файле таблицы импорта.

4.2 Функция get_imphash

Вычисляет значение imphash для PE-файла.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Значение imphash для PE-файла.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Таблица импорта отсутствует'): В случае отсутствия в PE-файле таблицы импорта.

4.3 Функция get_import_info

Возвращает информацию о таблице импорта PE-файла.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Информация о таблице импорта PE-файла в виде списка с элементами:

- имя импортируемой dll-библиотеки;
- список API-функций для каждой dll-библиотеки.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Таблица импорта отсутствует'): В случае отсутствия в PE-файле таблицы импорта.

CHAPTER 5

Модуль get_export_info

5.1 Функция get_export_api_num

Возвращает число экспортируемых функций.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Число экспортируемых PE-файлом функций.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Таблица экспорта отсутствует'): В случае отсутствия в PE-файле таблицы экспорта.

5.2 Функция get_export_dll_name

Возвращает имя библиотеки.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Строка с именем библиотеки.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Таблица экспорта отсутствует'): В случае отсутствия в PE-файле таблицы экспорта.

5.3 Функция get_export_info

Возвращает информацию о таблице экспорта PE-файла.

Аргументы:

- file_path - строка, содержащая путь PE-файлу.

Возвращаемое значение:

Информация об экспортируемых PE-файлом функциях в виде списка объектов типа dict с элементами:

- api - имя функции;
- ordinal - значение ординала (номера) экспортируемой функции;
- rva - значение RVA-адреса экспортируемой функции.

Исключения:

- PEfileScriptsError ('Запрашиваемый файл не найден'): В случае отсутствия проверяемого PE-файла.
- PEfileScriptsError ('Запрашиваемый файл не является PE-файлом'): В случае, когда проверяемый файл не является PE-файлом.
- PEfileScriptsError ('Таблица экспорта отсутствует'): В случае отсутствия в PE-файле таблицы экспорта.