

# Заражение 3G-модемов

# Модемы на рынке



E173



E171

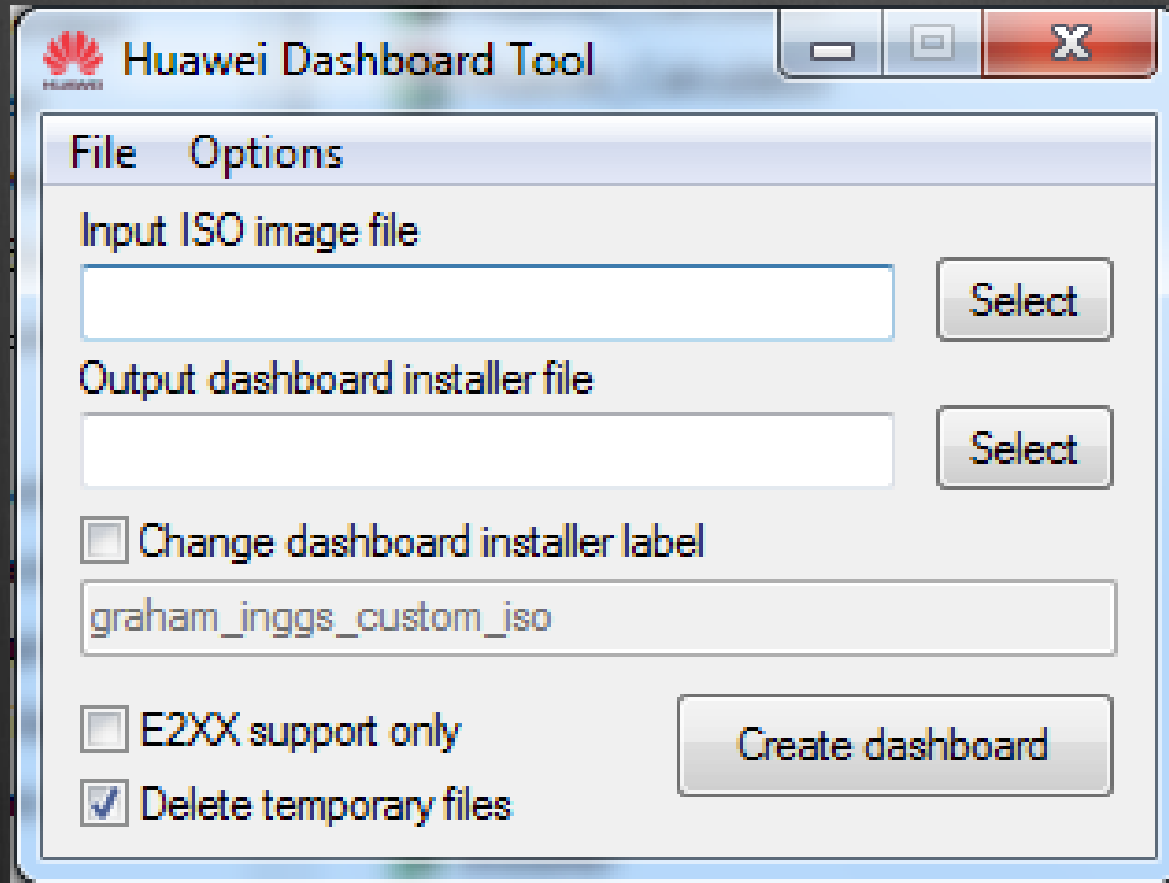


E171

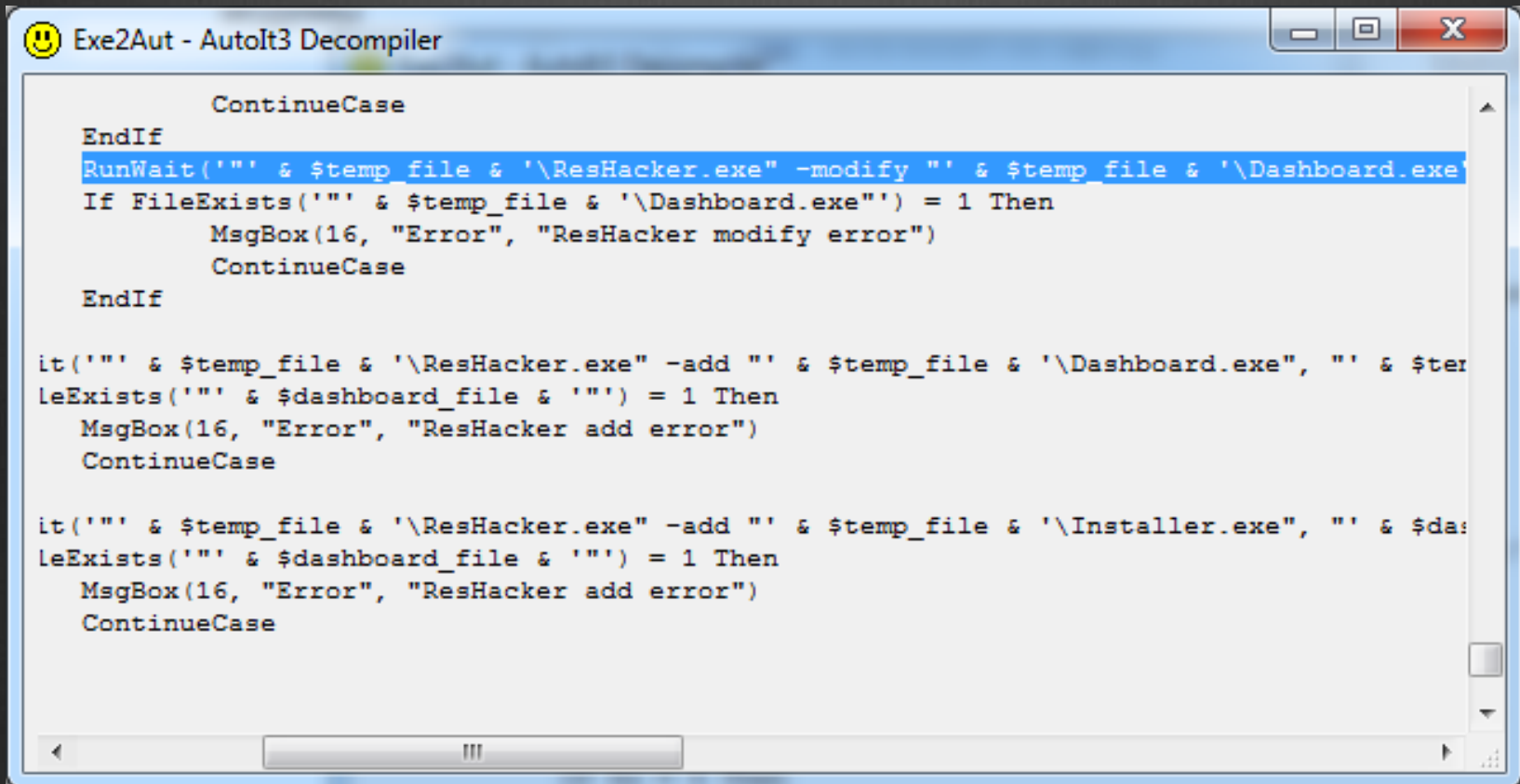
# Модели модемов

Оператор	Модем	Размер dashboard	Размер флеш
МТС	Huawei E171	52,7Mb	128Mb
Билайн	Huawei E171	49.7Mb	97Mb
Мегафон	Huawei E173	78,3Mb	97Mb

# Подарок от производителя



# Копнём немного глубже



The screenshot shows a window titled "Exe2Aut - AutoIt3 Decompiler" with a yellow smiley icon. The window contains a text editor with decompiled AutoIt3 code. The code is as follows:

```
ContinueCase
EndIf
RunWait('"' & $temp_file & '\ResHacker.exe" -modify "' & $temp_file & '\Dashboard.exe
If FileExists('"' & $temp_file & '\Dashboard.exe"' ) = 1 Then
    MsgBox(16, "Error", "ResHacker modify error")
    ContinueCase
EndIf

it('"' & $temp_file & '\ResHacker.exe" -add "' & $temp_file & '\Dashboard.exe", "' & $temp_file & '\Dashboard.exe"' ) = 1 Then
    MsgBox(16, "Error", "ResHacker add error")
    ContinueCase

it('"' & $temp_file & '\ResHacker.exe" -add "' & $temp_file & '\Installer.exe", "' & $temp_file & '\Installer.exe"' ) = 1 Then
    MsgBox(16, "Error", "ResHacker add error")
    ContinueCase
```

# Что заражать?

Операционная система	Файлы
Windows	\AutoRun.exe, \*modem*\Setup.exe, \*modem*\Data.bin
Linux	/autorun.sh, /install_linux
MacOS	/Connect Manager/Mobile Partner.app

# Вектор атаки

*Закр*ытый  
*во*енный объект



*Глупый кот*



# Зачем заражать?

- Проникновение на закрытые объекты, где интернет не положен по регламенту
- Интернет заблокировать проще, чем USB
- Возможность создания сборки: вирус+руткит+эксплойт к драйверам модема
- For fun 8)



# Защита

- Read-only dashboard
- Запрет на перепрошивку при вставленной сим-карте
- Other ideas?

# Приятные мелочи

- Отправка SMS на короткие номера
- Чтение SMS
- Убийство модема 8)