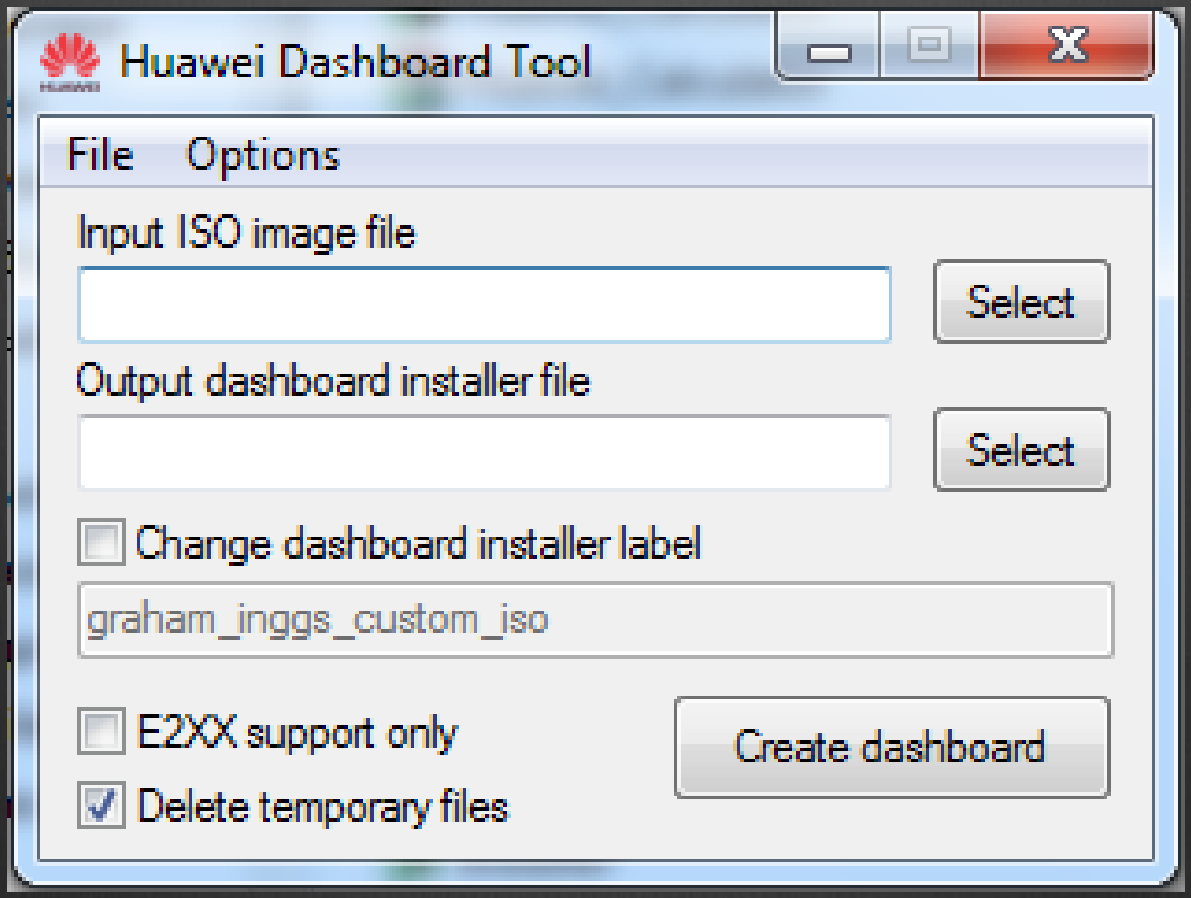
Заражение 3G-модемов

Модемы на рынке

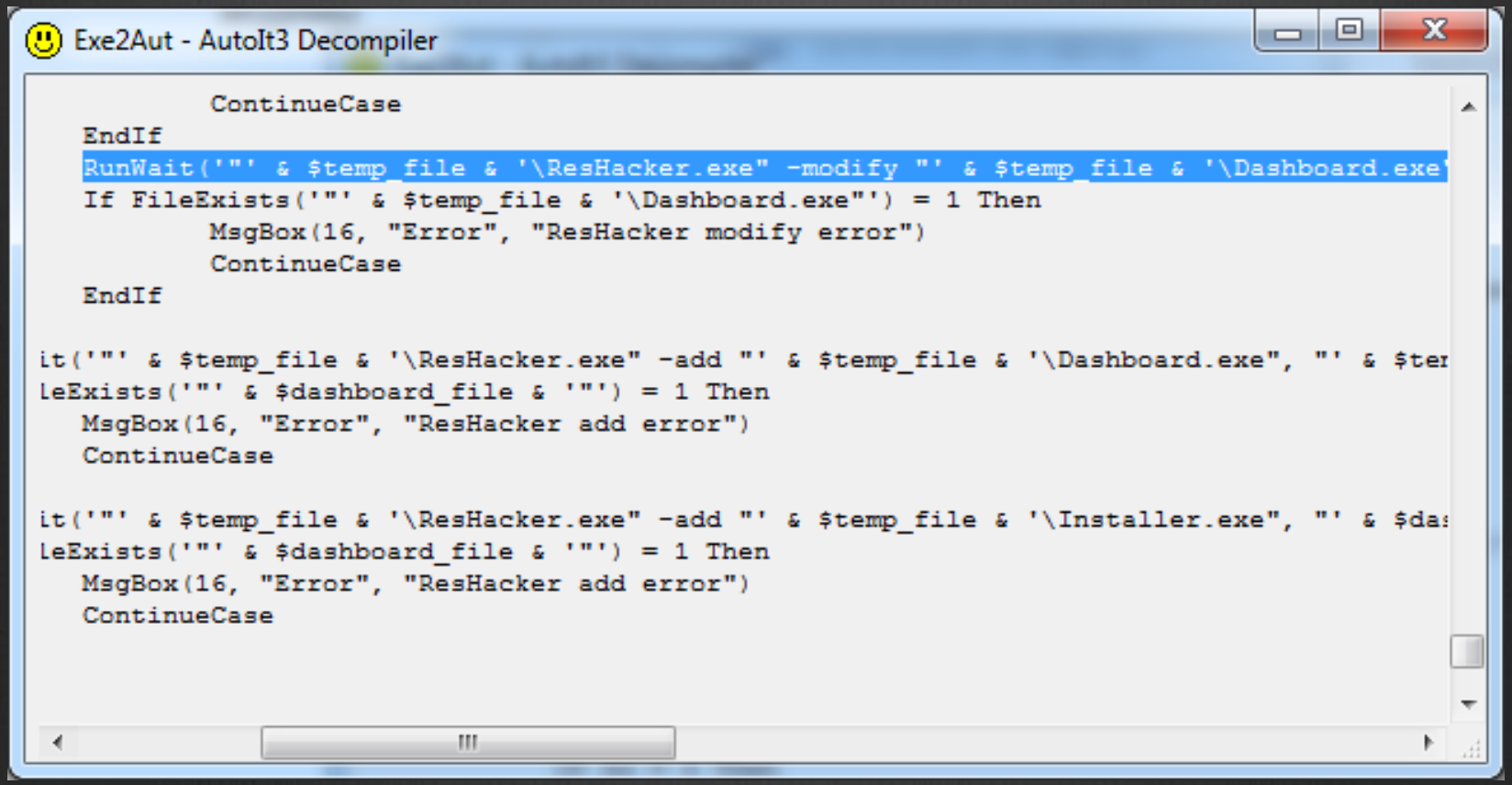
Модели модемов

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



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

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)