Перевод

Искусство распаковки. Потрошим защиту хитрого банкера GootKit

Malware Security * Reverse Engineering * Delphi * Software Cracking

Постоянно отслеживаю файлы, с целью не допустить попадания на компьютер. И что-то стало слишком часто попадаться подозрительное банкерное ПО. Вот, например, в последнем случае попадался подозрительный файлик, который, по мнению антивируса, был банкером. Ну, раз подозрительный, то и распаковать его нужно.

Intro

В предыдущей статье мы потрошили по-новому модифицированную версию, или для тонкости выражения, Smokeless v.0.12. Эта версия не отличается от предыдущей, поэтому, если вы не в курсе, то можете ознакомиться с ней.

Из интересующих нас будет использоваться только debug.exe (в Windows версии x32bit), которая входит в состав Microsoft Windows. Для 64-битных версий Windows 7x32 и выше также подойдет и приложение Debug.exe. Мы будем пользоваться, естественно, как самым распространенным и удобным в использовании приложением формата .com/.exe.

WARNING

Все манипуляции с этим файлом выполняются вручную, поэтому, если вы не знаете, что вы делаете, то лучше не делать. Также можно работать на основном компьютере, но лучше, все-таки, использовать для этого какую-нибудь виртуальную машину.

Для начала нужно конвертнуть из .com/.exe в .bin/.bin, для чего запускаем:

```
debug.exe -n -e -l -w -r -r -r
```