Итак, дорогие мои, представим что Вы обновились через Itunes 9 версии до прошивки 3.2.1 (этого нельзя делать потому что залочится если телефон у Вас родной или серый, я по доброте душевной так и сделал будучу уверенным что на такую подлость айтюнс не способен и мой родной айфон от at&t залочился) и у Вас всё встало колом потому что написано, что симка не поддерживается и всё такое, что делать Вы не знаете, никто не хочет за 1000 рублей сломать вам айфон потому что ещё не знает как ломать прошивку 3.2.1 и тут Вы понимаете что пришло время стать маленьким хакером-негодяем, нам будут нужны программы:

1)redsn0w-win_0.8
2)qickPWN225-2
3)quickPWN3RC
3)Прошивки для Iphone 3.2.1, 3.0.1, 3.0, 2.0.2
4)itunes 9

это всё добро можно взять на одном из моих сайтов:

http://91.195.252.70/iPhone/

Сразу оговорюсь, что суть этих действий: данугрейд до прошивки 3.0.1 и эксплуатация ошибки itunes 9 которая даёт нам право обойти lock в момент восстановления прошивки 3.0.1 с ошибкой 1604 и потом 1355 .

Когда мы всё скачали и отключили службу Apple mobile device в разделе служба в которую попали из панели управления нажав Пуск->Выполнить->Панель управления->Администрирование-> Службы делаем следующее, по пунктам:

0)Открываем программу quickPWN3 и выбираем прошивку 2.0.2 и пытаемся её залить, ничего не получается но прога нам нужна для включения recovery mode на телефоне, выключаем таким образом recovery mode и открываем itunes 9, который нам пишет, что нужно восстановить прошивку, отлично, выбираем прошивку 3.2.1 которую скачали, выбираем зажав shift около кнопки *восстановить* и восстанавливаем, всё отлично, телефон восстановлен до прошивки 3.2.1 после перезагрузки телефона нам говорят что у нас симка не та и телефон залочен, переходим к следующему шагу.
1)Запускаем redsnow и выбираем прошивку 3.0, устанавливаем используя инструкцию в окошке программы, которая раскажет как нам попасть в режим DFU на нашем айфоне, её, после ребута ничего не происходит, на экране провод и просьба подключить к itunes перезагружаемся, то же самое, всё залочено, открываем программу qickPWN3, выбираем прошивку 2.0.2 - вводим телефон в recovery mode после того как ввели телефон в recovery mode закрываем qickPWN3
2)Подключаем телефон к itunes, но он говорит нам что телефон в режиме восстановление и нужно бы его восстановить, выбираем прошивку 3.0 зажав shift около кнопки *восстановить* и выбрав из списка нашу прошивку, и восстанавливаем нажав *восстановить*, вылезает ошибка или 20 или 22 или 16, это нормально, закрываем Itunes

3)Открываем программу redsnow и восстанавливаем прошивку 3.0.1 руководствуясь инструкцией на экране, после перезагрузки такая же история, всё залочено, ничего не работает, открываем программу qickPWN и воодим телефон в режим восстановления выбрав ту же прошивку 2.0.1 то есть программа qickPWN3 нужна только для того чтобы быстро вводить наш айфон в recovery mode а она не сможет этого сделать без подходящей прошивки, такой алгоритм её работы
4)Подключаемся к itunes и он говорит нам что телефон в режиме восстановления, восстанавливаем прошивку 3.0.1 зажав shift и выбрав из списка прошивку 3.0.1 после чего нам вылезает ошибка 1604, закрываем itunes
5)Открывем программу qickPWN225-2 и смотрим что она просит нас сделать ребут телефона, делаем ребут двумя кнопками зажав Power и Home на 10 секунд это нужно для того, чтобы qickPWN225 смог попасть на iphone и перезагрузить его изнутри, буквально 5 секунд после ребута переходим к следубщему шагу, закрываем qickPWN225
6)Открываем программу qickPWN3 для того чтобы ввести телефон в режим восстановления, вводим в режим восстановления и закрываем quickPWN3
7)Снова подключаемся к itunesи пробуем восстановить прошивку 3.0.1, вылетает ошибка 1305 или ошибка 1355, закрываем itunes
8)Открываем программу redsnow и выбираем прошивку 3.0.1 и восстанавливаем выбрав прошивку 3.0.1, айфон не трогаем
9)Видим на экране изображение ананаса и отключаем телефон от компьюетра, затем выбираем оператора и язык
10)Пишем в комментах благодарности и спрашиваем если что-то непонятно.

Таким образом мы делаем:

1)Восстанавливаем 3.2.1
2)Восстанавливаем 3.0.1 получаем ошибку первый раз
3)Восстанавливаем 3.0 и получаем ошибку второй раз
4)Перезаливаем 3.0.1 через redwnow и всё работает

То есть все танцы с бубном нужны для того чтобы ввести itunes 9 в ступор который нам позволит между пунктом 3 и 4 влить свою прошивку и эксплуатировать непонятную ошибку которая не позволяет лочится нашей прелести. Если говорить научным языком, то мы просто под прошивку 3.2.1 вливаем окружение ядра от 3.0.1 в момент когда происходит сбой itunes и то есть мы имеем у себя мутировавший в следствии грязного хака гибрид прошивок 3.2.1 и 3.0.1 то есть по факту у нас 3.2.1 ядро и окружение 3.0.1.

Если что то не получилось делаем весь список сначала, я проверял три раза последовательность - всё работает, убил два дня.

P.s. сразу хочу сказать что я не несу ответственности если у Вас что-то поломается.
Tags: apple

Оригинал http://zingelll.livejournal.com/66012.html

{jcomments on}