

PSP Hacking



Saludos a los amigos de la comunidad y a demás lectores. En esta ocasión haré un artículo sobre como hackear nuestra PSP (ya sea la antigua PSP Fat o la nueva Slim) sin exploits, es decir, usando el nuevo truco de la Bateria Pandora. Esto para cargarle un Custom Firmware y así poder ejecutar homebrew. El tutorial también sirve para reparar las PSP's brickeadas.

Requisitos:

- Una PSP FAT con Custom Firmware (2.xx o 3.xx).
- Una Memory Stick PRO Duo Sony o SanDisk de 256MB o más.
- Los archivos “MSO”, “MSPFormat” y “MSInst” (Mirrors anexos al final)
- Una PC con Windows o bien *Linux con WINE (método aún no probado)*
- Conector MiniUSB o lector de tarjetas Memory Stick PRO Duo en el PC

NOTA IMPOTANTE:

Lee bien el tutorial antes de atreverte a hacerlo, no me hago responsable por daños o perdidas de datos en tu consola.

Pasos:

Creando la Magic Memory Stick

- Formatea la Memory Stick en tu PSP FAT con Custom Firmware.
- Conecta el PSP con el cable al PC y ponlo en Modo de Conexión USB o bien, inserta la memoria en el lector de tu PC. En Linux, monta el PSP o la memoria en “\$USER/.wine/drive_g”.
- Descomprime los archivos MSPFormat, MSInst y MSO.
- En Windows, ve a Inicio > Ejecutar > CMD y ejecuta el mspformat con el parametro g (donde g es la letra donde esta el PSP o la Memory Stick). En Linux abre una terminal y ejecuta “wine /ruta-de-mspformat.exe g” (*No he podido probar este metodo*). Podemos ver la siguiente pantalla para saber si ha tenido

exito la operación.

```
C:\ C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\leobardo>cd..
C:\Documents and Settings>cd..
C:\>cd mspformat
C:\mspformat>mspformat.exe h
You are about to format the drive h.
All data will be lost. Do you want to continue? [Y]y
Drive succesfully formatted, and partition moved.
C:\mspformat>_
```

- Ahora sin apagar tu PSP retira la memoria y sal del modo USB (si lo hiciste por USB), ahora vuelve a insertar la memoria y entra de nuevo al modo USB, vuelve a montar si es necesario (en Linux). Ahora copia todo el contenido de MSO a la Memory Stick, debería quedar así:



- Sal del modo USB (y si no tenias la memoria en el PSP insertala) y ahora en el PSP ve a Game/Juego > Memory Stick > Despertar del Cementerio y sigue las instrucciones.
- Ahora vuelve al modo USB del PSP (o conecta tu memoria en el PC) y copia el archivo msipl que ya habias descomprimido a la carpeta MSINST y en el CMD (o con Wine en la terminal) ejecuta el “msinst.exe” para que quede así: msinst.exe g msipl.bin (recuerda que g es en Windows la unidad donde esta tu PSP), te saldrá lo siguiente:

```
ca C:\WINDOWS\system32\cmd.exe - msinst.exe h msipl.bin
C:\Documents and Settings>cd..
C:\>cd msinst
G:\msinst>msinst.exe h msipl.bin
PSP MS IPL Installer
Load IPL code msipl.bin
241664 bytes(59 block) readed
Target DRIVE is 3
Check partation Sector
boot status      0x80
start head      0x01
start sec/cyl   0x0001
partation type  0x0E
last head       0x7F
last sec/cyl   0xC9E0
abs sector     0x00000810
ttl sector     0x003C97F0
signature      0xAA55
Check BPB Sector
signature       AA55
Check free reserved sector:OK
Write ABS Sector 0x10 to 0x1E?
Are You Sure ?[Y]
```

- Ahora ya tienes lista la Magic Memory Stick. Lo siguiente es crear la Bateria Pandora.

Creando la Bateria Pandora

- En el PSP ve a Game/Juego > Memory Stick > Pandora's battery Creator
- Presiona Triangulo para resparlar tu EEPROM
- Vuelve a ejecutar el Pandora's Battery Creator, pero esta vez presiona X para crear la Bateria de Pandora (En la sección de consideraciones se menciona como volverla a su estado normal).

Desbrickeando/Hackeando el PSP para instalar el CUSTOM Firmware.

- Ahora en el PSP que queremos desbrickear o hackear insertamos la Bateria Pandora y lo encendemos (sin la Memory Stick). Una vez encendido, insertamos la Memory Stick.
- 1.- Presiona x para instalar el custom firmware 3.71m33 (OPCION RECOMENDADA)
- 2.- Preciona círculo para instalar el original 3.71 de sony
- 3.- Preciona cuadro para hacer un dump de tu nand del psp.
- 4.- Preciona L+R+start para restaurar el nand dump(muy peligroso).
- Con esto nuestra PSP queda lista

CONSIDERACIONES MUY IMPORTANTES.

- No debemos intentar convertir la bateria del PSP Slim a Pandora ya que quedaría dañada.
- Para restaurar una Bateria Pandora a su estado normal, en nuestro PSP con Custom Firmware ejecutamos Game/Juego > Memory Stick > Pandora's battery

Creator pero en esta ocasión presionamos cuadrado.

- No he probado el método en Linux, pero pueden ver actualizaciones sobre el tema en el foro o bien en mi blog (<http://okltsmash.blogspot.com>).
- Si tenemos una PSP FAT que queríamos hackear o desbrickear, es necesario si le instalamos el CUSTOM FIRMWARE ejecutar en Game/Juego > Memory Stick > 150kernel_addon2. El PSP debe tener mas del 78% de carga para realizar esto.
- Carga la batería completamente antes de seguir el tutorial.

Glosario

- *Brick*: Una "PSP brickeada", es una consola que ha tenido un error grave en el momento del downgrade del firmware, o un virus de extensión realmene escasa. Este fallo prácticamente irreparable (*sólo es reparable con el UP*) y no está cubierto por la garantía de la SCE (*Sony Computer Entertainment*)
- *Dump / Dumpeo*: Significa volcar, descargar. Un claro ejemplo es volcar el contenido de un UMD en la Memory Stick contenida en la PSP, con objeto de realizar un Backup, para luego poder ejecutarlo.
- *Firmware*: El firmware es el software que hace funcionar el hardware de nuestra PSP. Con actualizaciones de firmware se pueden conseguir implementar mas funciones (*o recortarlas*) en la PSP. El firmware tiene el poder, de permitir o no, que un programa sea ejecutable. En el caso de la PSP, Sony implementa en los firms más recientes una firma digital que impide ejecutar software casero.
- *Homebrew*: Software hecho en casa, de programas y utilidades realizadas por la scene sin ningún tipo de apoyo oficial.
- *Kernel*: Núcleo de un sistema operativo. El gran objetivo de Sony es tapar fallos de seguridad en la PSP con cada una de sus actualizaciones. De esta forma bloquea el acceso al modo Kernel, imposibilitando la ejecución de software casero.

Mirrors para Descarga de los Archivos

- MSO: <http://rapidshare.com/files/60706408/MS0.rar>
- MSInst y MSFORMAT:
http://rapidshare.com/files/59860183/msinst_y_mspformat.rar

De momento es todo. Proximamente veremos como instalar algo de homebrew en nuestro PSP (Emuladores, otros Sistemas Operativos, etc).

Tutorial de Leo_Fox readaptado y ampliado por LTSmash