Subject: "No Gameplay Pending" patch for LFDS!
Posted by howang on Sun, 08 Oct 2006 14:25:30 GMT
View Forum Message <> Reply to Message

After a few days of work and much help from BadBoy, I've found out the way to patch the LFDS for always "Gameplay in process". This is my first reserve engineering product, and the experience is great! If there is anything wrong, please tell me so that I can have a chance to improve.

RH7.3
==========
offset xxxxx | org | new
offset 23A38 | B8 | 90
offset 23A39 | 87 | B8
offset 23A3A | F8 | 01
offset 23A3B | 01 | 00
offset 3FECA | 00 | 01
==========

Special thanks to:
StealthEye for the initial idea on patching the cGameDataCnc::Is_Gameplay_Permitted(void)
v00d00 for the wFDS version patch
BadBoy for finding out sub_472C40 = cGameData::Export_Tier_1_Data(cPacket &) and explain the tricks in the wFDS version patch

P.S. I'll find out the offsets in the RH8 version of LFDS soon

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by Cat998 on Sun, 08 Oct 2006 15:40:25 GMT
View Forum Message <> Reply to Message

well done mate !

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by howang on Sun, 08 Oct 2006 17:14:07 GMT
View Forum Message <> Reply to Message

Cat998 wrote on Sun, 08 October 2006 23:40well done mate !
ty

besides, I think I've found the bytes for RH8, it is quite tricky because it works in another way that is difference from the RH7.3 version and the wFDS

offset xxxxx | org | new
offset 2BBAA | B8 | 90
offset 2BBAB | 87 | 90
offset 2BBAC | F8 | 90
offset 2BBAD | 01 | 90
offset 2BBAE | 01 | 6A
offset 2BBAF | 01 | 01
offset 3DF12 | 00 | 01

I don't have a box to run the RH8 version, anyone can help me to test it?

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by Blazer on Tue, 10 Oct 2006 23:31:49 GMT
View Forum Message <> Reply to Message

I run the RH8 version. Are you manually patching or are you using a tool or script?

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by howang on Wed, 11 Oct 2006 00:46:07 GMT
View Forum Message <> Reply to Message

I patched it with a hex editor and upload it to the server for testing.
After the patch works, I deleted the "excess" patched binary and patch the unpatched version with a patcher program, which is modified from the patcher.c from the scripts.dll/scripts.so package.

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by Blazer on Wed, 11 Oct 2006 02:22:12 GMT
View Forum Message <> Reply to Message

I'll test your patcher.c on my RH8 binary...then you can release it!

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by howang on Wed, 11 Oct 2006 05:08:12 GMT
View Forum Message <> Reply to Message

/* * * * * * * * * * * * * * *
LFDS no gameplay pending patcher (RH7.3)

offset xxxxx | org | new
offset 23A38 | B8 | 90
offset 23A39 | 87 | B8
offset 23A3A | F8 | 01

```
offset 23A3B | 01  | 00
offset 3FECA | 00  | 01
* * * * * * * * * * * * * * * */

#include <stdio.h>
#include <stdlib.h>

int main(int argc, char* argv[])
{
 FILE *f;
 printf("Renegade LFDS no gameplay pending patcher\n");
 if (argc < 2)
 {
  printf("Usage: patcher <name of Linux FDS binary>\n");
  exit(1);
 }
 f = fopen(argv[1],"rb");
 if (f == 0)
 {
  printf("File %s not found\n",argv[1]);
  exit(1);
 }
 fclose(f);
 printf("patching Redhat 7.3 binary\n");
 char c;
 f = fopen(argv[1],"r+b");
 fseek(f,0x23A38,SEEK_SET);
 c = 0x90; /* 0x90 is a big cheater */
 fwrite(&c,1,1,f);
 fseek(f,0x23A39,SEEK_SET);
 c = 0xB8;
 fwrite(&c,1,1,f);
 fseek(f,0x23A3A,SEEK_SET);
 c = 0x01;
 fwrite(&c,1,1,f);
 fseek(f,0x23A3B,SEEK_SET);
 c = 0x00;
 fwrite(&c,1,1,f);
 fseek(f,0x3FECA,SEEK_SET);
 c = 0x01;
 fwrite(&c,1,1,f);
 printf("Patching complete\n");
}

/* * * * * * * * * * * * * * *
LFDS no gameplay pending patcher (RH8.0)

offset xxxxx | org | new
```

```
offset 2BBAA | B8 | 90
offset 2BBAB | 87 | 90
offset 2BBAC | F8 | 90
offset 2BBAD | 01 | 90
offset 2BBAE | 01 | 6A
offset 2BBAF | 01 | 01
offset 3DF12 | 00 | 01
* * * * * * * * * * * * * * * */

#include <stdio.h>
#include <stdlib.h>

int main(int argc, char* argv[])
{
 FILE *f;
 printf("Renegade LFDS no gameplay pending patcher\n");
 if (argc < 2)
 {
  printf("Usage: patcher <name of Linux FDS binary>\n");
  exit(1);
 }
 f = fopen(argv[1],"rb");
 if (f == 0)
 {
  printf("File %s not found\n",argv[1]);
  exit(1);
 }
 fclose(f);
 printf("patching Redhat 8.0 binary\n");
 char c;
 f = fopen(argv[1],"r+b");
 c = 0x90; /* 0x90 is a big cheater */
 fseek(f,0x2BBAA,SEEK_SET);
 fwrite(&c,1,1,f);
 fseek(f,0x2BBAB,SEEK_SET);
 fwrite(&c,1,1,f);
 fseek(f,0x2BBAC,SEEK_SET);
 fwrite(&c,1,1,f);
 fseek(f,0x2BBAD,SEEK_SET);
 fwrite(&c,1,1,f);
 c = 0x6A;
 fseek(f,0x2BBAE,SEEK_SET);
 fwrite(&c,1,1,f);
 c = 0x01;
 fseek(f,0x2BBAF,SEEK_SET);
 fwrite(&c,1,1,f);
 fseek(f,0x3DF12,SEEK_SET);
 fwrite(&c,1,1,f);
```

```
 printf("Patching complete\n");
}
```

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by Stumpy on Fri, 13 Oct 2006 16:23:06 GMT
View Forum Message <> Reply to Message

Nice work howyang
I dont think that everyone knows how compile works so..
I link the compiled version with Source Readme.txt so that everyone can use it.
http://ren-hq.de/files/rh8.zip
http://ren-hq.de/files/rh7.zip

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by howang on Sun, 15 Oct 2006 02:33:30 GMT
View Forum Message <> Reply to Message

UESir28:
that's C but not C++
btw, did you test the rh8 version for me? it's syntax should be correct, but I don't know if it work or not.

Yes, I forgot to post the command for compile and run it:
gcc -o gameplay_in_process_patcher <name of the C file>
chmod a+x gameplay_in_process_patcher
./gameplay_in_process_patcher <name of LFDS binary>

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by Stumpy on Sun, 15 Oct 2006 09:26:10 GMT
View Forum Message <> Reply to Message

yes i tested it its working fine.

Subject: Re: "No Gameplay Pending" patch for LFDS!
Posted by howang on Mon, 16 Oct 2006 00:33:31 GMT
View Forum Message <> Reply to Message

Thank you UESir28.

So now, it is safe for everyone to use the patch!