

Forum:[Hack Forums](#)

Thread: [FBI Money Pak Virus popping up in all safe modes](#)

XxFoRMxX - February 6, 2013, 5:10 pm

Got a client with a computer with the FBI Money Pak virus. Typically I boot a computer infected with that virus into safe mode with networking, manually remove the virus exe and startup entry, then run full scans with SuperAntiSpyware and MalwareBytes Anti-Malware.

Now when I try to boot the computer into safe mode with networking, the same message appears and I am unable to access windows explorer to navigate to the infection to delete it. The same message appears in safe mode with command prompt and plain jane safe mode. I am unable to boot the recovery partition.

Am I going to have to reinstall the operating system from the OEM DVD-ROM, or is there something I'm not getting?

Dubai - February 6, 2013, 5:11 pm

Just do a factory reset and wipe all viruses , etc. Just hope there was nothing important on your hard drive. Or just back it up on an external hard drive just in case (while it has infected files) and wipe the system.

Scottdos - February 6, 2013, 5:26 pm

Should not be starting up in safe mode it appears the virus has managed to modify safe-reg values which allowed it to enter into safe mode, can possibly allow the program to fully disable it! a recent virus has been spotted in the wild capable of completely ridding the OS of safe mode, requiring a fresh install to rid of it.

#Reliant - February 15, 2013, 7:19 pm

My laptop had that and I went to repair computer, luckily my laptop auto backups once a year and I had just done a backup.

ÇdnîS Lu?i? - March 3, 2013, 11:03 pm

Ive removed this before... It has access to admin rights. The new virus is located in System 32 and in Startup. Lsass.exe bans admin rights but restarts the virus Ctfmon.exe. Im stumped =O

SHADOW REALM - March 3, 2013, 11:06 pm

Download Hiren's boot cd, boot from a cd/usb then you can go and delete the actual files

And then when you boot back into normal windows you can remove the registry files

ÇdnîS Lu?i? - March 4, 2013, 4:05 pm

Ive tried puppy linux and even that has no access to modify NTFS only read access. I will try your method.

ÇdnîS Lu?i? - March 5, 2013, 9:49 pm

I have solved the problem. If anyone needs assistance pm me and i will gladly walk you thru the tedious procedure i used. I don't have time to post it atm =X