

# Re: Root kits ...lully !

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2006-06/msg00053.html>

---

- *From:* "RJK" <[notatospam@xxxxxxxxxxx](mailto:notatospam@xxxxxxxxxxx)>
  - *Date:* Sat, 10 Jun 2006 12:41:58 +0100
- 

Well ! ...seeing as the NTFS4DOS bootable floppy (made by the wizard included with it), doesn't boot up properly, I made a bootable floppy from my XP Home ed. SP2 system, and copied the ntfs4dos.exe, its' other \*.exe's ....chkdsk.exe, 2 x defrag files onto it, in case I needed them.

I booted up with it, (lovely – now I'm told I'm booting from floppy into Windows Millenium [Version 4.90.3000] !!  
I ran ntfs4dos and I can see all my drives ! BUT the keyboard and character tables are all wrong and haven't been loaded correctly – I can't type a tilde, in order to type startm~.bat ! So I suppose now I've got to tweak config.sys / country.sys and autoexec.bat on floppy, and fiddle with keyb.exe and mode.exe and CHCP437 etc. ...moan ....moan.. that I haven't had to tweak for AGES ! :-) ...I can't remember all that syntax ! ...God ! MS will have me digging out my old copy of Quarterdeck in a minute !

regards, Richard

"RJK" <[notatospam@xxxxxxxxxxx](mailto:notatospam@xxxxxxxxxxx)> wrote in message  
[news:%236djcp7iGHA.4044@xxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%236djcp7iGHA.4044@xxxxxxxxxxxxxxxxxxxxxxxxxxx)

Thanks Leythos

I can already do that i.e. – boot to Safe Mode and copy the multi-av directory onto a c:\drive etc.. What I was trying to do was, boot from floppy, or bootable cd-r using Freedos such as that in NTFS4DOS, so that I'm in an OS that definately hasn't been "hooked," and then run multi-av, or the seperate command line scanners, (that I haven't yet collected), that will also be burnt to cd-r, ...copy them onto C:\ etc. and work at a DOS prompt.

While experimenting, one thing that's puzzling me, is that after booting up from the NTFS4DOS bootable floppy, it take AGES to boot up – eventually I get a colourful screen asking me if I'm using it for private or business use, where I have to type in "yes" and hit [Enter], and I'm left with no access to hd partitions i.e. only drives A:\ and C:\ (a ramdrive) are accessible at the DOS prompt.

...oh well ...continuing to fiddle :-)

Re: Root kits ...lully !

regards, Richard

"Leythos" <void@xxxxxxxxxxx> wrote in message  
[news:s1cig.41933\\$YI5.21778@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:s1cig.41933$YI5.21778@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

In article <eCOviw6iGHA.4276@xxxxxxxxxxxxxxxxxxxxxxxxxxx>,  
notatospam@xxxxxxxxxxx says...

..one thing that crosses my mind when using with DOS level  
progs. (such  
as  
multi-av), is "Oh dear – no ide/bus master drivers in use i.e.  
data  
stream  
down to a crawl \ on the ribbons !"

How would one boot from bootable-cd to a clean DOS os /  
or XP "Safe  
Mode"  
that loaded IDE drivers – and then could run multi-av a lot  
faster ? :-)

When I use Multi-AV, I download it to a clean machine, run all the  
updates, burn the entire folder to a CD, and then take it to the machine  
to be cleaned – boot in safe mode, copy the CD folder to the C:\  
location (so that the folder is copied) and then run the different  
scanners from the menu.

--

spam999free@xxxxxxxxxxx  
remove 999 in order to email me