

Re: Boot virus & root kit?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2006-09/msg05367.html>

- *From:* "Richard Urban" <richardurbanREMOVETHIS@xxxxxxxxxxxxx>
 - *Date:* Sun, 17 Sep 2006 07:56:25 -0400
-

A root kit will NOT survive a partition delete/create/format/install routine.

And, I have not seen a boot sector virus for over 10 years (doesn't mean that a new one has not been released).

Sacrifice your system and start completely fresh.

--

Regards,

Richard Urban
Microsoft MVP Windows Shell/User
(For email, remove the obvious from my address)

Quote from George Ankner:
If you knew as much as you think you know,
You would realize that you don't know what you thought you knew!

"JM" <[artmoore\(at\)nbnet.nb.ca](mailto:artmoore(at)nbnet.nb.ca)> wrote in message
news:u86H1gk2GHA.1256@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello,
I contacted you last week concerning a boot virus and you directed me to "drive scrubber"(nice product)
problem is that even with a 7 hr complete wipe, I still have the virus.I have unplugged my machine and removed the battery and all memory overnight and cleared the cmos
when i reinstall windows xp (any version)on this HDD the same thing happensFor about five minutes after connecting to the net everything is fine .. then all of a sudden i cannot connect (even though my connection is showing active) i tried to scan with various online scanners but it wont let me download them giving me various error messages ..I have even tried loading full virus protection from a cd (norton internet security 2006)but it stopped the live update process.... same with trend micro, this virus is STEALTH and after about 20 min the pc

Re: Boot virus & root kit?

basically locks up. and cpu is overworking . also you cannot set the drive as slave and scan because the virus will infect the master drive (already happened)I took my pc to another repair technician and he didn't want to hook it up to his.(He has no idea either) I did some research and i believe i have a root kit virus .. there is a program on the net called "ICESWORD" that detects rootkit virus but i do not know how to use the program and it has no instructions with it .Its found on the sysinternals site.If anyone has any info on this type of virus and how to remove it please contact me in this form .. i have 2 HDD down and a 6 gig travel drive that i cannot use
after a week im running out of ideas nothing shows up in Hyjack this . cannot download virus software in safe mode with networking &