

NTFS design flaw?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-04/0261.html

From: Robert Jones (robert@altalang.com)

Date: 04/03/03

From: "Robert Jones" <robert@altalang.com>

Date: Wed, 2 Apr 2003 17:04:06 -0800

You have a virus. The virus loads immediately AFTER the master boot record has been read. You can't go online. You can't access other boot modes because the virus has infected some key OS files.

How do you remove it?

What doesn't work:

- 1) boot floppy (after reading the boot record on the floppy, the system must access the HD drive to load the OS, and thus loads the virus)
- 2) Windows XP CD (The recovery console is useless unless you know exactly which file(s) have been infected.
- 3) You can't go online.
- 4) Virus scans won't load because of virus countermeasures.
- 5) Boot CDs from Norton and others can't access NTFS partitions.
- 6) Reinstalling the XP will erase user settings and deletes the contents of My Documents (according to the XP setup screen)

Is the only option to Repair the OS?

Under Win95 and Win98 this was an easy problem to solve, but now???