

# Booting From Floppy Causes Windows 2000 to Reinstall SP4?

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-12/msg00080.html>

---

- *From:* "Will" <[westes-usc@xxxxxxxxxxxxxxxxx](mailto:westes-usc@xxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 27 Dec 2006 00:58:10 -0800
- 

We have a system that we are sure has been infected by some kind of rootkit or stealthy virus. For reasons unrelated to the virus, we booted off a Windows 2000 boot floppy to this system. What happened is something I have never seen before and I want to better understand the behavior.

Windows 2000 started to boot and immediately came up and asked us to insert the SP4 CD. At that point the Windows installer took over and started to run through the final stages of a Windows 2000 upgrade. It's just a pure guess, but maybe the virus had replaced the boot sector or some of the critical system files, and when we booted off a not-infected Windows 2000 boot floppy, that path detected the modified files, interpreted this as "corruption", and started a re-install? What kind of checksum verifications is the Windows 2000 kernel doing on startup?

Can someone explain what the startup logic in Windows 2000 is and what the behavior I am describing means? We'll test tomorrow to see if this re-install did anything to remove the virus from the system.

—

Will

.