

## RE: system32 "invisible" system.driv deleted

---

*Source:*

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2005-07/msg00760.html>

---

- *From:* PATOPP <[PATOPP@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:PATOPP@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 15 Jul 2005 05:46:03 -0700
- 

It turns out, this was Malware utilizing a rootkit. According to [http://www.kpmginsiders.com/display\\_analysis.asp?action=vote&cs\\_id=135509](http://www.kpmginsiders.com/display_analysis.asp?action=vote&cs_id=135509) "The term "rootkit" stems from the Unix operating system, in which the highest level of administrative permissions is called "root access." A rootkit is software that grants a user advanced privileges, such as the ability to hide files or applications from the rest of the operating system. In the Windows operating environment, rootkits can conceal spyware, viruses, keystroke loggers, and other malicious software. In the worst instances, the malware can promote identity theft by capturing user identities and passwords."

This particular instance was hiding my system32 folder and system.driv (along with other 'system' files. I discovered this while trying to rename a file with DOS to system.driv and it stated that the file already existed. I could not (as administrator) even grant myself permissions or ownership of certain areas of my drive.

THE FIX! I had new virus signatures, but an older engine. I had to remove my drive and put it in to another computer as a secondary drive. The other computer had a new virus scan engine and new signatures. It was able to remove the rootkit and once installed back into its original box, the anti-spyware programs were able to clean the malware. I hope this post helps someone.

"PATOPP" wrote:

> 2000 Pro. When starting an old 'voice-mail' program, I get a system.driv file  
> is missing or corrupt, please reinstall. In my search for the system.driv  
> file, I discovered that my system32 folder is hidden and unsearchable from  
> explorer. Even at a command prompt, the dir command won't reveal the  
> directory. I can, however, 'cd' to the directory and 'dir' its contents.  
> Sure enough, no system.driv file exists. When I try to copy or expand  
> system.driv from a cab file, it is immediately deleted from my system. I  
> suspect a virus, but with the latest signatures, nothing shows. I've ran the  
> new versions of spybot and adaware with their respective, new signatures and  
> cleaned off all items that show. Throughout this, I am unable to make my  
> system32 folder visable and searchable again. I have tried the attrib -h on  
> the folder at the commanc prompt. I have ran sfc /scan now, but nothing was  
> fixed. Where else should I be looking and what else could I do? (I would

RE: system32 "invisible" system.drv deleted

- > like to upgrade to XP Pro– but I want to do that with a functioning version
- > of 2K, so I don't drag problems into XP) Thank you for any help, I know
- > you've helped me before, in this group.
- > PATOPP

.

- 
- Prev by Date: [\*Re: Looking for Indexing Software\*](#)
  - Next by Date: [\*Windows 2000 computer frequently cannot log into Domain\*](#)
  - Previous by thread: [\*Simple question – I hope\*](#)
  - Next by thread: [\*Windows 2000 computer frequently cannot log into Domain\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)