

comp.security.firewalls: Re: Someone look at this HijackThis log, please?

## Re: Someone look at this HijackThis log, please?

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-12/0530.html>

---

*ss\_spa\_at\_hotmail.com*

*Date:* 12/09/03

Date: Tue, 09 Dec 2003 10:52:30 -0800

On Tue, 09 Dec 2003 14:56:23 GMT, Aly929@nospam.net (Allen) wrote:

>Logfile of HijackThis v1.95.1  
>Scan saved at 14:48:44, on 09/12/03  
>Platform: Windows 98 SE (Win9x 4.10.2222A)  
>MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)  
>  
>C:\WINDOWS\SYSTEM\mmtask.tsk

some kind of spyware maybe?

>C:\WINDOWS\SYSTEM\QTTASK.EXE

Quicktime. You don't need this running all the time. Start MSCONFIG from Start/Run, click on theStartup tab and uncheck this.

>D:\WINUTILS\CD-RW\CLONECD\CLONECDTRAY.EXE

CloneCD. You don't need this running all the time. Start MSCONFIG from Start/Run, click on theStartup tab and uncheck this.

>C:\PROGRAM FILES\COMMON FILES\REAL\UPDATE\_OB\REALSCHED.EXE

Real Audio. You don't need this running all the time. Start MSCONFIG from Start/Run, click on theStartup tab and uncheck this. Also start Real Audio, and uncheck the option to do automatic updates.

>C:\WINDOWS\SYSTEM\IEDRIVER\IEDRIVER.EXE

Adware.Get Adaware, or Spybot Search and Destroy.

>C:\PROGRAM FILES\SAVE\SAVE.EXE

Adware.Get Adaware, or Spybot Search and Destroy.

>C:\PROGRAM FILES\COMMONNAME\ADDRESSBAR\WINNET.EXE

Re: Someone look at this HijackThis log, please?

comp.security.firewalls: Re: Someone look at this HijackThis log, please?

Adware. Get Adaware, or Spybot Search and Destroy.

>D:\WINUTILS\CAPSWARN\CAPHK.EXE

Definitely don't need this. You don't need this running all the time.  
Start MSCONFIG from Start/Run, click on theStartup tab and uncheck  
this.

>C:\PROGRAM FILES\CLOCKSYNC\SYNC.EXE

Adware. Get Adaware, or Spybot Search and Destroy.

>C:\PROGRAM FILES\COMMONNAME\ADDRESSBAR\COMWIZ.EXE

More adware/spyware.

You may also wish to grab a copy of Spyware Blaster.  
You should also learn how to harden IE against drive by downloads and  
other nasties.

tim