Subject: "mstinit.exe"
Posted by IRON FART on Sat, 17 Apr 2004 22:09:24 GMT
View Forum Message <> Reply to Message

I did a Google search on "mstinit.exe" because today I have been getting rid of some worms on my computer, and some dialers/trojans/hijackers from my "system32" folder.

As you can see from the google search, "mstinit.exe" (10KB) is indeed some sort of spyware or hijacker.

So naturally, I Shift+Delete it. Exactly 5 seconds later, another one appears.

Great...

This suggests that there is another program that is checking to see if it is present, and if not, it is replaced. So I made a copy of "notepad.exe" (50KB), renamed it to "mstinit.exe" and replaced the original. This works. This make file is not replaced by the original 10KB file. However, If I delete this new file, it is replaced by a copy of the fake, 50KB file.

So this other program is still present. Taskmanager says otherwise...

```
Logfile of HijackThis v1.97.7
Scan saved at 3:02:58 PM, on 4/17/2004
Platform: Windows 2000 SP4 (WinNT 5.00.2195)
MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

Running processes:
C:\WINNT\System32\smss.exe
C:\WINNT\system32\winlogon.exe
C:\WINNT\system32\services.exe
C:\WINNT\system32\lsass.exe
C:\WINNT\system32\svchost.exe
C:\WINNT\system32\spoolsv.exe
C:\Program Files\Apache Group\Apache2\bin\Apache.exe
D:\AVG6\avgserv.exe
C:\WINNT\system32\svchost.exe
C:\Program Files\Apache Group\Apache2\bin\Apache.exe
C:\MYSQL\BIN\MYSQLD-NT.exe
C:\WINNT\system32\nvsvc32.exe
C:\WINNT\system32\regsvc.exe
C:\WINNT\system32\MSTask.exe
C:\WINNT\system32\stisvc.exe
C:\WINNT\System32\WBEM\WinMgmt.exe
C:\WINNT\system32\svchost.exe
C:\WINNT\Explorer.EXE
C:\PROGRA~1\PESTPA~1\PPControl.exe
C:\PROGRA~1\PESTPA~1\PPMemCheck.exe
C:\PROGRA~1\PESTPA~1\CookiePatrol.exe
```

```
D:\AVG6\avgcc32.exe
C:\WINNT\system32\RUNDLL32.EXE
C:\Program Files\AIM\aim.exe
C:\Program Files\Hewlett-Packard\AiO\hp psc 700 series\Bin\hpobrt07.exe
C:\Program Files\Apache Group\Apache2\bin\ApacheMonitor.exe
C:\mysql\bin\winmysqladmin.exe
C:\PROGRA~1\HEWLET~1\AiO\Shared\Bin\hpoevm07.exe
C:\WINNT\system32\hpoipm07.exe
C:\Program Files\Hewlett-Packard\AiO\Shared\bin\hpOSTS07.exe
C:\Program Files\Internet Explorer\IEXPLORE.EXE
C:\Program Files\Internet Explorer\IEXPLORE.EXE
```

I scanned my computer with:
http://housecall.trendmicro.com
AVG 6.0
Adaware 6
Pest Patrol
Hijack This

And none of them picked up on the original "mstinit.exe" as a threat. And the application that is causing this wasn't found either. There is no reference to this file at http://www.symantec.com or http://us.mcafee.com.

I'm not getting any adverse effects of this file (its just a clone of notepad.exe) and I can operate my computer fully, but I still don't want this or my other file on my computer.

TIA

Subject: "mstinit.exe"
Posted by Adnecles1 on Sat, 17 Apr 2004 22:20:11 GMT
View Forum Message <> Reply to Message

download a program called spybots and update before running it. It looks for all kinds of spyware/adware.

Subject: "mstinit.exe"
Posted by mrpirate on Sat, 17 Apr 2004 22:40:12 GMT
View Forum Message <> Reply to Message

It doesn't look like a trojan/spyware to me.

Subject: "mstinit.exe"

Posted by Javaxcx on Sat, 17 Apr 2004 23:01:49 GMT
View Forum Message <> Reply to Message

I had a similar problem with a gaobot variant. Norton would go into crazy mode, but couldn't repair the file "soundman.exe". So I would delete it, only to have it respawn again at a random interval later on.

What I assumed was that if it was an outsider trying use my computer, I could simply block him out by disabling my DMZ. If you have a router, check and see if your DMZ is open -- and if it is, close it. That solved my problem.

Subject: "mstinit.exe"
Posted by IRON FART on Sat, 17 Apr 2004 23:28:16 GMT
View Forum Message <> Reply to Message

No, disabling DMZ didn't do it. Neither did disabling forwarding.

And I searched with SpybotSD (nice little app). It fixed some other problems etc... But didn't find anything relating to the cause of this file spawning.

Subject: "mstinit.exe"
Posted by Javaxcx on Sat, 17 Apr 2004 23:30:55 GMT
View Forum Message <> Reply to Message

Well, it might just be possible that your file might not be written remotely like mine was. You can do a couple of things, check your connections, run>cmd>netstat.exe for any IPs that shouldn't be there (just a precaution) or check your processes. If there is anything running which shouldn't be running, close it, and track it down.

Subject: "mstinit.exe"
Posted by IRON FART on Sun, 18 Apr 2004 00:08:26 GMT
View Forum Message <> Reply to Message

Well, I found out what the problem is. And I restored the original file.

mstinit.exe is the Windows Task Scheduler Setup. I don't know what it does.

But it occured to me after I restored it from the W2K CD that it was actually the Windows File protection restoring the file to its original state.

Oh well, no harm done at least.

Thanks for the help
It is appreciated.