

comp.security.misc: Re: Software Registry: is "Advanced INF" legit Explorer?

## Re: Software Registry: is "Advanced INF" legit Explorer?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2005-10/0125.html>

---

**From:** Carey Frisch [MVP] ([cnfrisch\\_at\\_nospamgmail.com](mailto:cnfrisch_at_nospamgmail.com))

**Date:** 10/07/05

Date: Thu, 6 Oct 2005 18:53:56 -0500

Unexplained computer behavior may be caused by deceptive software

<http://support.microsoft.com/?-id=827315>

Download Ad-aware SE and scan your PC for the presence of spyware:

<http://www.download.com/3000-2144-10045910.html?part=69274&subj=dlpage&tag=button>

Symantec Security Check

<http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym&plfid=23&pkj=RRJXPKXYSHMSPCSIZME>

Microsoft Windows AntiSpyware

<http://www.microsoft.com/downloads/details.aspx?FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&displaylan>

Here's what you can do to enhance the security on your PC

<http://www.microsoft.com/athome/security/protect/windowsxpsp2/Default.msp>

--

Carey Frisch  
Microsoft MVP  
Windows XP - Shell/User  
Microsoft Newsgroups

-----  
"Michelle" wrote:

| Lately I've been having a lot of adware entering the system, trying to  
| install the common round of searchbars, popups and the like. There's  
| been a number of attempts to hijack the Internet Explorer startpage,  
| and I know at some points the msieexec.exe process has been used for  
| this ( i haven't modified the browser myself or installed any MS  
| updates for some time). I try to keep the malware at bay with Norton  
| Firewall /Antivirus, Adaware and so far I've avoided really grave  
| attacks.

| The other day I had a look at the registry and deleted some keys that  
| were obvious adware, but registry is a place where you need to know  
| exactly what you're doing and I'm not a software pro...

| Now, next I found dozens of keys under the line HKEY\_LOCAL\_MACHINE  
| Software\Microsoft\Advanced INF Setup. Some seemed limited in scope and  
| not really part of the ordinary Internet Explorer registry. I ran a  
| registry scan afterwards with Norton and had it delete a few other keys  
| I was positive was adware. Tonight, when I just checked the registry  
| again, some of these suspect keys I'd spotted seemed to be gone, others  
| still there. Although they were stored under Microsoft, this would be

comp.security.misc: Re: Software Registry: is "Advanced INF" legit Explorer?

| an ordinary spot for any intruding adware, wouldn't it? Is this  
| (HKEY\_LOCAL\_MACHINE Software\Microsoft\Advanced INF Setup) a default  
| registry class for matters dealing with integration of Explorer with  
| different kinds of multimedia, or is it a place primarily "used" to  
| lodge spyware and adware? And just what does "Advanced INF" mean here?

| Hope to get enlightened on this,  
| /Michelle

| Main software specs:

| Windows XP Pro + Service Pack 1  
| Internet Explorer 6  
| Opera 7 (second browser)  
| Acrobat 6 Pro & Acrobat Reader