

Re: System Restore

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-11/2730.html

From: Rick \ (rick_at_mvps.org)

Date: 11/08/04

Date: Sun, 7 Nov 2004 21:41:11 -0500

Hi,

Two instances of spyware:

```
"ViewMgr"="C:\\Program Files\\Viewpoint\\Viewpoint Manager\\ViewMgr.exe"  
"WildTangent CDA"="RUNDLL32.exe \\\"C:\\Program  
Files\\WildTangent\\Apps\\CDA\\cdaEngine0400.dll\\",cdaEngineMain"
```

But no viruses. What makes you think that you have one?

--

```
Best of Luck,  
Rick Rogers, aka "Nutcass" - Microsoft MVP  
http://mvp.support.microsoft.com/  
Associate Expert - WindowsXP Expert Zone  
www.microsoft.com/windowsxp/expertzone  
Windows help - www.rickrogers.org  
"Fishslayer" <Fishslayer@discussions.microsoft.com> wrote in message  
news:FCE1A1DA-F4B0-4723-8822-A9AE30ABAED6@microsoft.com...  
> Here's what I found...thanks for your help!!!  
> Windows Registry Editor Version 5.00  
>  
> [HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run]  
> "Sonic RecordNow!"=""  
> "MSMSG"="\\\"C:\\Program Files\\Messenger\\msmsgs.exe\\\" /background"  
>  
>  
> [HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run]  
> "NvCplDaemon"="RUNDLL32.EXE C:\\\\WINDOWS\\System32\\NvCpl.dll,NvStartup"  
> "BCMSMSG"="BCMSMSG.exe"  
> "dla"="C:\\\\WINDOWS\\system32\\dla\\tfswctrl.exe"  
> "StorageGuard"="\\\"C:\\Program Files\\Common Files\\Sonic\\Update  
> Manager\\sgtray.exe\\\" /r"  
> "DVDSEntry"="C:\\\\WINDOWS\\System32\\DSEntry.exe"  
> "diagent"="\\\"C:\\Program  
> Files\\Creative\\SBLive\\Diagnostics\\diagent.exe\\"  
> startup"  
> "UpdReg"="C:\\\\WINDOWS\\UpdReg.EXE"  
> "TkBellExe"="\\\"C:\\Program Files\\Common  
> Files\\Real\\Update_OB\\realsched.exe\\\" -osboot"  
> "VSOCheckTask"="\\\"c:\\PROGRA~1\\mcafee.com\\vso\\mcmnhdlr.exe\\"  
> /checktask"  
> "MCAgentExe"="c:\\PROGRA~1\\mcafee.com\\agent\\mcagent.exe"
```

microsoft.public.windowsxp.help_and_support: Re: System Restore

```
> "MCUpdateExe"="C:\\PROGRA~1\\McAfee.com\\Agent\\mcupdate.exe"
> "VirusScan Online"="\"c:\\PROGRA~1\\mcafee.com\\vso\\mcvsshld.exe\"
> "DwlClient"="C:\\Program Files\\Common Files\\Dell\\EUSW\\Support.exe"
> "Dell AIO Printer A920"="\"C:\\Program Files\\Dell AIO Printer
> A920\\dlbkbmgr.exe\"
> "PLoader"="c:\\program files\\pendrive tools english version\\pendrive.exe
> sys_auto_run C:\\Program Files\\PENDRIVE Tools English Version"
> "QuickTime Task"="\"C:\\Program
> Files\\QuickTime\\qttask.exe\" -atboottime"
> "ViewMgr"="C:\\Program Files\\Viewpoint\\Viewpoint Manager\\ViewMgr.exe"
> "WildTangent CDA"="RUNDLL32.exe \"C:\\Program
> Files\\WildTangent\\Apps\\CDA\\cdaEngine0400.dll\",cdaEngineMain"
> "MPFExe"="C:\\PROGRA~1\\McAfee.com\\PERSON~1\\MpfTray.exe"
> "iTunesHelper"="C:\\Program Files\\iTunes\\iTunesHelper.exe"
>
>
> When I tried to pull up the string :
> HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Shared Tools\\MSConfig\\startupreg
> there
> wasn't anything under MsConfig. The only items available with an "M"
> were:
> MSInfo; MSWinWrite; MSWord6.wpc and MSWord8
>
> I hope this is what you were looking for...I'm not that technical. and
> I've
> never been in the registry before. Thanks "Nutcase"!
>
> Fishslayer
>
>
> "Rick "Nutcase" Rogers" wrote:
>
>> Hi,
>>
>> Click start/run, type regedit and click ok. Export a copy of the
>> following
>> keys:
>>
>> HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
>> HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
>> HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Shared Tools\\MSConfig\\startupreg
>>
>> Right click each of the keys in turn, choose edit. Then copy/paste the
>> contents of each into a reply.
>>
>> --
>> Best of Luck,
>>
>> Rick Rogers, aka "Nutcase" - Microsoft MVP
>> http://mvp.support.microsoft.com/
>> Associate Expert - WindowsXP Expert Zone
>> www.microsoft.com/windowsxp/expertzone
>> Windows help - www.rickrogers.org
>>
>> "Fishslayer" <Fishslayer@discussions.microsoft.com> wrote in message
>> news:79509126-54F3-4BE7-AA44-816256910071@microsoft.com...
>> > I finally managed to get in as the Administrator!! I ran the Stinger,
>> > under the repair option, and rebooted my computer. Nothing has really
>> > changed. When I go into Outlook, my email program immediately attempts
>> > to
>> > send 55 emails. I don't know what else to do to get rid of the virus.
>> > McAfee is of little help!! I've tried Spybot, Ad-Aware SE and Kaspersky
```

microsoft.public.windowsxp.help_and_support: Re: System Restore

```
>> > virus
>> > removal programs to identify and disable the virus...but none seem to
>> > work.
>> > Any programs that you would recommend? Thanks for your help, it is
>> > much
>> > appreciated!!
>> >
>> > "Fishslayer" wrote:
>> >
>> >> Thanks "Nutcase". I downloaded the Stinger program, but it is under
>> >> my
>> >> username, and not the Administrator. When I try to get into safemode,
>> >> I
>> >> keep
>> >> getting a "Key Board Failure" which won't allow me to type in the
>> >> password as
>> >> the Administrator. I can get into Safe Mode...just not as the
>> >> Administrator,
>> >> and the Stinger tool is not listed as one of the programs from which
>> >> to
>> >> choose. Any suggestions? This is frustrating!!
>> >>
>> >> "Rick "Nutcase" Rogers" wrote:
>> >>
>> >>> Hi,
>> >>>
>> >>> If the restore points are infected, then going back is pointless. If
>> >>> they
>> >>> are corrupted and System Restore fails, then there is no going back.
>> >>>
>> >>> Suggest instead you download stinger from
>> >>> http://vil.nai.com/vil/stinger/
>> >>> and then restart in Safe mode. Logon as administrator, then run the
>> >>> file
>> >>> where it won't be interfered with by the virus.
>> >>>
>> >>> How to start in Safe mode:
>> >>> http://www.rickrogers.org/fixes.htm#Safe%20mode
>> >>>
>> >>> --
>> >>> Best of Luck,
>> >>>
>> >>> Rick Rogers, aka "Nutcase" - Microsoft MVP
>> >>> http://mvp.support.microsoft.com/
>> >>> Associate Expert - WindowsXP Expert Zone
>> >>> www.microsoft.com/windowsxp/expertzone
>> >>> Windows help - www.rickrogers.org
>> >>>
>> >>> "Fishslayer" <Fishslayer@discussions.microsoft.com> wrote in message
>> >>> news:5ADB18F6-2135-4931-BEB0-606930AD5D2D@microsoft.com...
>> >>> >I can't go back in time with system restore due to a
>> >>> >trojan/virus/worm
>> >>> >that
>> >>> >> has infected my computer. McAfee can't seem to identify/remove
>> >>> >> the
>> >>> >> virus
>> >>> >> and
>> >>> >> I'd like to go back in time to a previous setting. Help please.
>> >>> >> Thanks
>> >>> >
>> >>> >
>> >>> >
```

microsoft.public.windowsxp.help_and_support: Re: System Restore

>>
>>
>>