

Win32_StartupCommand lists \system32 files

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.wmi/2005-05/msg00094.htm>

- *From:* Tom <cogitator_x@xxxxxxxxxxxxxxx>
 - *Date:* Fri, 13 May 2005 15:48:35 GMT
-

A Google search found someone else reported this problem a while back, but no searches I've done have found any cause, or solution, for the \root\CIMV2 Win32_StartupCommand problem where we get back a list of all the files in our \system32 folder (in **addition** to the expected data).

Background:

I have a fairly comprehensive WMI-based JScript I've been running on 315 (mostly Dell, but not all) computers where I work, since January, and the information coming back from the various WMI queries have been expected and correct.

One my own stand-alone, not in a domain, workstations is an Alienware Athlon64-based system running XPsp2 (installed with our SP2-level campus agreement media).

My last archived output file shows this computer had the **expected output** to the Win32_StartupCommand query as of May 2, 2005. However, at some point in the past few days, I noticed this problem. All of my other 300+ computers still return the expected data.

Problem:

The Win32_StartupCommand query not only returns the expected data (the currently logged-in users's entries in the \Startup folder, the HKU Run registry key, the All Users's \Startup folder and the HLKM Run key),

but now **ALSO** returns a "Startup" entry for all of the \system32 files (>2072) for **BOTH** User ".DEFAULT" and again for User "NT AUTHORITY\SYSTEM".

In other words, 4000+ extra entries are being returned by the Win32_StartupCommand query, on this one computer, starting sometime after May 2.

Win32_StartupCommand lists \system32 files

Anyone have *any* ideas? The only change to the system I can think of, around the time this problem started, I had installed the SQL Server Express Edition April CTP and Visual Web Developer 2005 Express Edition Beta 2. I've subsequently removed those, and all previously installed Visual Studio applications, as well as the .NET 2.0 beta. It would seem logical that this would have been the cause, but I don't have the time to do the proper methodical testing to prove or disprove it.

I reinstalled WMI, per these instructions:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/reinstalling_wmi.asp

The problem persists, however.

I've enabled WMI logging and don't see anything suspicious, but I also don't claim to be an expert on all things low-level WMI. If there is something specific I should look for, please let me know.

The code I use for the WMI queries, as I mention above, works on over 300 computers and as has for the last five months. To rule out any code oddities that could somehow affect only one computer, out of the blue, I verified the same bizarre output when running Microsoft's Scriptomatic v2 app.

I also ran the WMI script remotely, from an older Dell NT5.0 workstation, and it returned the same extra, unwanted data.

--

Output snippet from Scriptomatic v2 (JScript),
for the \root\CIMV2 Win32_StartupCommand query:

Caption: \$winnt\$
Command: \$winnt\$.inf
Description: \$winnt\$
Location: Startup
Name: \$winnt\$
SettingID: null
User: NT AUTHORITY\SYSTEM
.... continues for all \system32 files

--

Caption: \$winnt\$
Command: \$winnt\$.inf
Description: \$winnt\$
Location: Startup
Name: \$winnt\$
SettingID: null
User: .DEFAULT

.... continues for all \system32 files

-
- Prev by Date: ***Re: Non-Admin access to Win32 DiskDrive, Win32 PNPEntity***
 - Next by Date: ***RE: Data retrieval questions***
 - Previous by thread: ***Non-Admin access to Win32 DiskDrive, Win32 PNPEntity***
 - Next by thread: ***wmi and DCOM launch permissions***
 - Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***