Charles Sestokas
Lexington Computer and Technology Group Oct 28, 2015

Potpourri - Win 10 stuff being loaded/installed on Win 7 and Win 8.1 computers

Disclaimer – Last Week; Newsletters, Qs on today's topic

This week – Potpourri on

- Win 10 Install Kits being loaded on Win 7 and Win 8.1 Computers

- MS "snooping" on Win 7 and Win 8.1 Computers (like in Win 10)

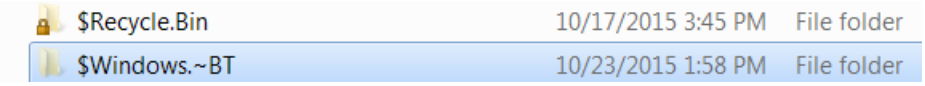
"Win 7, Win 8.1 Users need be aware of Win 10 stuff being forced on You"

- Win 10 Install Kits being loaded on Win 7 and Win 8.1 Computers

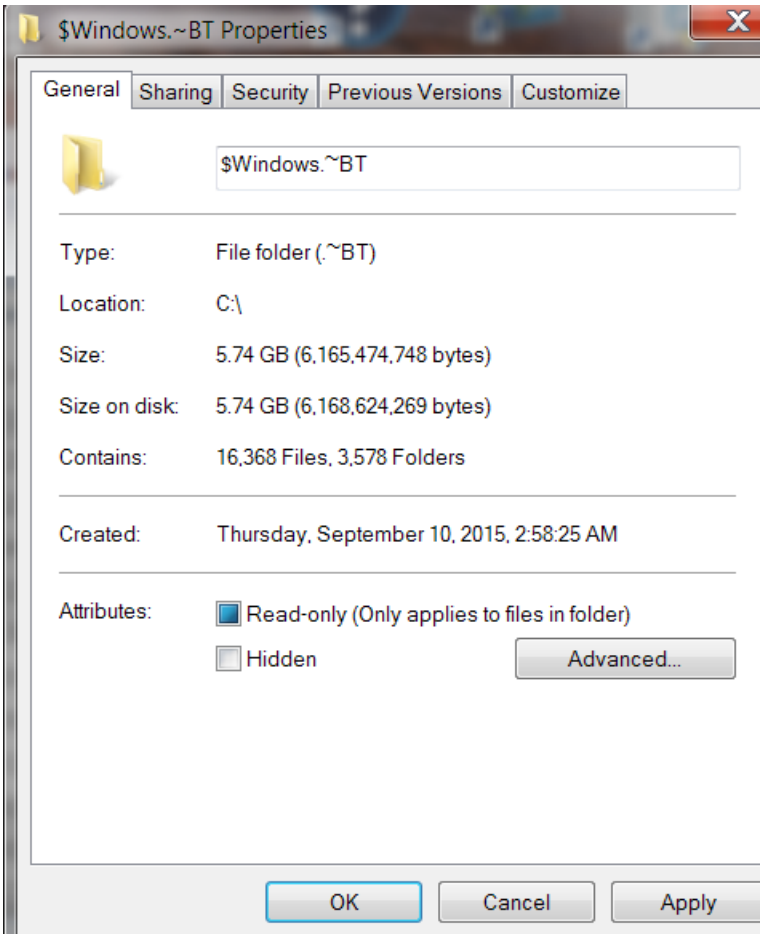
ref: **"GWX Control Panel" to disable the auto-upgrade to Win10**

Windows 10 Upgrade NAGS become more Aggressive, offer NO OPT-OUT
by Adrian Kingsley-Hughes Oct 15, 2015

***** Some Windows 7 and Windows 8.1 users are finding that they can only reschedule and NOT CANCEL Windows 10 upgrades.**



find *** In Hidden < $Windows.~BT> Folder ~4gb for Home, ~5.8gb for Pro



and YOU **didn't even ask**, never mind allow this

If will migrate to the FREE Win 10 Upgrade, then do Nothing !

If Unsure, or will NOT migrate to FREE Win 10 Upgrade,

then need "GWX Control Panel" from: http://ultimateoutsider.com/downloads/
to disable the auto-upgrade to Win10. More info at: http://blog.ultimateoutsider.com/

http://blog.ultimateoutsider.com/2015/08/using-gwx-stopper-to-permanently-remove.html

Using GWX Control Panel (formerly GWX Stopper)
to Permanently Remove the 'Get Windows 10' Icon

{ GWX = **G**et **W**indows 10 ie **X** = Roman 10}

GWX Control Panel (previously named GWX Stopper) is a free program that you can use to configure and exit the "Get Windows 10" system tray application which continually pops up on PCs that are still running Windows 7 and Windows 8.
It can also prevent unintentional Windows 10 upgrades from occurring via Windows Update. GWX Control Panel really works, is safe and easy to use, and gives you the option to re-enable the icon and upgrade notifications if you're ever ready to move forward with Windows 10.

UPDATE (October 20, 2015): Version 1.4 is now live. This fixes some of the more stubborn Windows Update issues folks have reported and *hopefully* finally fixes the dreaded Windows 10 "reschedule or upgrade now" cycle that some users have found themselves in.

Disk Space Issue

Any other Qs on this ?

- MS "snooping" on Win 7 and Win 8.1 Computers (like in Win 10)

If will migrate to the FREE Win 10 Upgrade, then do Nothing !

http://windowssecrets.com/top-story/attempting-to-answer-whether-ms-is-snooping/

Attempting to answer whether MS is snooping

By Susan Bradley on October 1, 2015 in Top Story

Microsoft has recently released updates to Windows 7 that allow it to gather more information about our PCs.

But is the company really tracking what we do on our systems? And can this data gathering be turned off?

Backporting Win10 telemetry tools to Win7/8.1

What Microsoft built into Windows 10 from the start, it recently added to our Win7 and Win8.1 systems via a series of updates. (That's caused quite a tizzy in the blogosphere, with most of the "discussions" based on conjecture and hearsay.) For example, optional KBs 3075249, 3080149 and 3068708 give Win7 and Win8.1 data-gathering capabilities similar to Win10's.

If you have automatic updating turned off (as I have frequently recommended) you can ignore or hide those updates. But Microsoft has a habit of changing the status of some optional updates, moving them to the Important section in Windows Update and setting them as prechecked.

An alternative to constantly checking these "optional" telemetry updates is to turn off the telemetry services altogether. Windows Secret's sister publication — Windows IT Pro — provides advanced-user instructions for disabling the Windows Tracking Service; see the Sept. 9 article, "How to: Turn off telemetry in Windows 7, 8, and Windows 10." This technique will ensure you don't have to hide future telemetry updates.

But, again, there's a potential price to pay: Turning off telemetry in Windows could slow the pace of operating-system fixes. Moreover, this trick doesn't necessarily turn off ***all*** system tracking.

Other attempts to track telemetry transmissions

Another way to block Internet connections is the HOST-file technique (more info), which works for Win7 and Win8.1. However, on Windows 10, some users tried that trick to block telemetry communications, but, as noted on several websites — including an Aug. 31 Ars Technica story — Microsoft's telemetry system simply ignores the HOST-file method. In a big change from Win7, you must take ownership of the HOST file in order to make changes in the new OS.

My attempts at Windows 7 telemetry analysis were based on steps posted by software developer Rob Seder, who was investigating his Win10 machine. Following his instructions, I used Wireshark to log transmissions from Win7 to the following websites:

- vortex-win.data.microsoft.com
- settings-win.data.microsoft.com
- cs1.wpc.v0cdn.net
- df.telemetry.microsoft.com
- i1.services.social.microsoft.com
- i1.services.social.microsoft.com.nsatc.net
- oca.telemetry.microsoft.com
- oca.telemetry.microsoft.com.nsatc.net
- pre.footprintpredict.com
- reports.wes.df.telemetry.microsoft.com
- sqm.telemetry.microsoft.com
- sqm.telemetry.microsoft.com.nsatc.net
- statsfe1.ws.microsoft.com
- telecommand.telemetry.microsoft.com
- telecommand.telemetry.microsoft.com.nsatc.net
- telemetry.appex.bing.net
- telemetry.urs.microsoft.com
- vortex-sandbox.data.microsoft.com
- vortex-win.data.microsoft.com
- vortex.data.microsoft.com

Although most of the urls in that list appear to be subdomains of Microsoft, a few, such as **pre.footprintpredict.com,** are related to the Bing search engine, as noted on the VirusTotal website.

An even longer list of MS telemetry-related urls, posted on the MajorGeeks site, includes domain names such as **akadns.net,** which is attached to the Akamai content delivery network service. Large companies such as Microsoft often offload some Web duties to services that specialize in secure content delivery over the Internet.

I left Wireshark running overnight. In the morning, it was clear that the Windows telemetry system hadn't "phoned home" often. And, again, the information sent to Microsoft was mostly unreadable by the network-analysis software (see Figure 1).

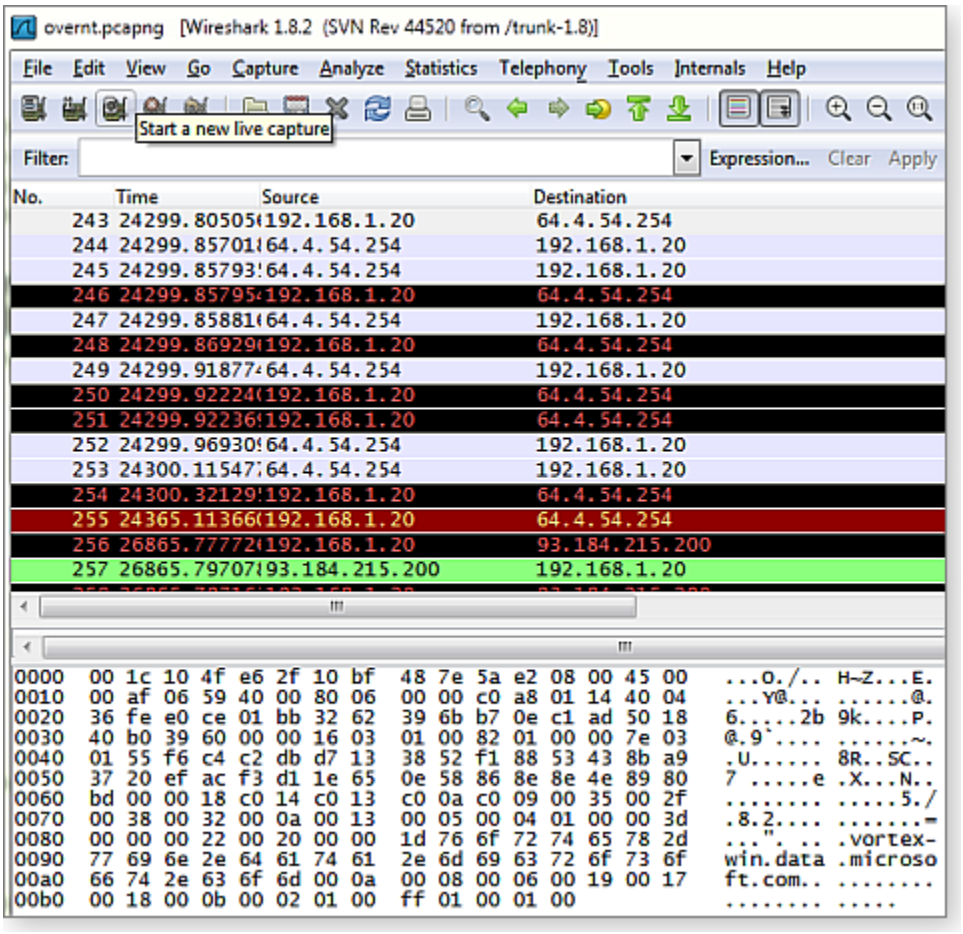


Figure 1. The results of my Wireshark analysis of Windows telemetry data

The 'Everyone does it, so it's okay' argument

Read the privacy policies of nearly every major Web service, and you might want to return to paper cups and string for your daily transmissions. Microsoft's privacy policy raises numerous concerns, but in truth it's not any worse than Google's or Apple's policies. They all say that they give you control over your privacy, but none say what they collect in any detail or in a way that the average human can interpret.

That's not really acceptable. Most of us are willing to provide personal information to Web services — for mapping, searching, sharing, and so forth — for a better computing experience. But what happens to that information, now that it resides on Internet servers? Many users assume it's deleted when we no longer need it; but, in fact, we simply don't know. And that's what we should be most concerned about — the lack of transparency.

The difficult decisions for personal privacy

I started this investigation to see whether I could determine exactly what information Microsoft is gathering from my systems. I was pleased that this telemetry data is now protected — but I was also disappointed that I couldn't answer my primary question: Is Microsoft snooping on us?

Based on Microsoft's privacy policy and a recent Blogging Windows post by Windows honcho Terry Meyerson, I'm fairly comfortable that the telemetry information won't be used for truly malicious intent; hackers can't access and use the information to wage attacks on our systems.

But there's also the "Big Data" aspect. Will that data make its way to other massive services and get combined with other sources of information about us? I recently attended a technology conference that discussed Big Data services, and I came away both impressed and worried.

Still, as noted in a recent ZDNet article, if you've gone through Win10's numerous privacy settings and you're still uncomfortable about what the company does with your data, the alternative is to not upgrade to the new OS — or use "Chrome OS, iOS, Android, or any other system that's tied closely into the cloud."

I'm not ready to chuck those platforms, and I assume you aren't either. But that doesn't mean we should blindly accept vendors' data-gathering practices.

On Windows 7 and 8.1 systems, you have fewer privacy options. Here, I recommend disabling the Windows telemetry service. Neither OS will see significant enhancements, so we're mostly concerned with all-important security updates.

Open the start menu and click Administrative Tools/Services (or Control Panel/Administrative Tools/Services). Scroll down the list of services until you find **Diagnostic Tracking Service.** Click it and stop the service, then click OK. Now right-click the service and open Properties. Change **Startup type** from Automatic to **Disabled** (see Figure 2) and then click OK. (Note: If you don't see the service, it's probably because you're behind a domain and didn't get optional updates KB 3075249, KB 3080149, and KB 3068708 installed, install that service.)

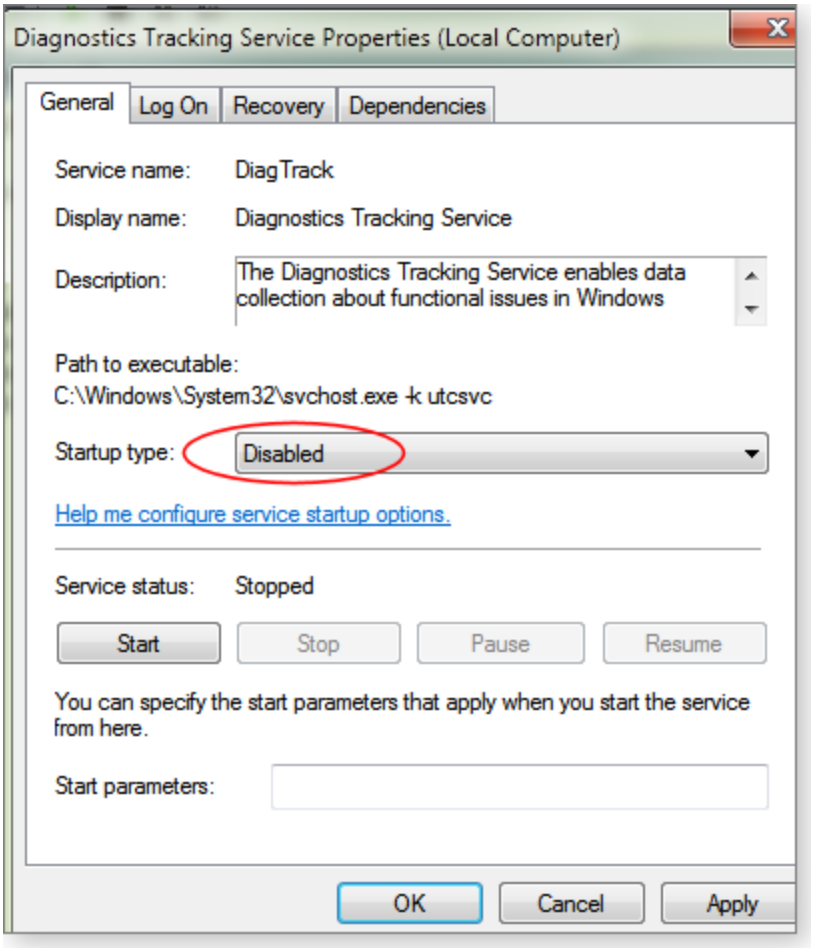


Figure 2. You can reduce the data your Win7 or Win8.1 system sends back to Microsoft by disabling Windows' Diagnostic Tracking Service.

I'm keeping the service disabled on my Win7 (and probably my Win10 systems, too),

until I find out exactly what is being sent to Microsoft

— or I feel more comfortable with the telemetry process.

And I'm keeping a closer eye on all other Web-attached services and software.