

Re: Windows Genuine Advantage – Big Brother is watching you

Re: Windows Genuine Advantage – Big Brother is watching you

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2006-06/msg00976.html>

- *From:* "Stefaan" <me2@xxxxxxxxxxxx>
 - *Date:* Sun, 18 Jun 2006 22:21:36 GMT
-

"Carey Frisch [MVP]" <cnfrisch@xxxxxxxxxxxxxxxx> schreef in bericht
<news:OjU%23f68jGHA.3588@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Please read the following and become informed:

Microsoft Provides Additional Clarity About Windows Genuine Advantage Notifications
<http://www.microsoft.com/presspass/features/2006/jun06/06-08wgaqa.mspx>

"read my lips: I did not have s*x with that woman"

Shame on you, MSFT, lying about this disgraceful "Genuine unwanted beta Disadvantage"
to honest paying customers like myself.

Whatever a lip-syncing MVP is posting here,
WGA is one of the worst mistakes MSFT made in 2006.

Time to "become informed" indeed:

<http://windowssecrets.com/comp/060615/#story1>

Quote from the URL above:

—

Windows Genuine Advantage is Microsoft spyware

By Brian Livingston

Re: Windows Genuine Advantage – Big Brother is watching you

Re: Windows Genuine Advantage – Big Brother is watching you

Windows Genuine Advantage the controversial program Microsoft auto-installed as a "critical security update" on many PCs starting on Apr. 25 not only causes problems for many users but has now been proven to send personally identifiable information back to Redmond every 24 hours.

This behavior clearly fits any plausible definition of "spyware." Some tech writers have said categorizing WGA as spyware is arguable. But I have no hesitation in calling the program a security nightmare that Microsoft should never have distributed in its present form.

In my May 25 newsletter, I called Microsoft's WGA download a "severe blunder." It causes serious problems for some legitimate Windows users and was sprung on customers with no notice other than a press release the day before.

No PC-using company that values security and reliability can allow a program like WGA to send data to a distant server, download additional software, morph its behavior, or remotely change the functionality of Windows (as I describe below). I don't believe individuals should put up with this, either.

Today, I'll explain the problems and let you know what you can do to fix them.

If the spyware label fits, wear it

In a statement released on June 8, Microsoft officially denies that WGA is spyware. Let's settle this question right off the bat so we can quickly move on to more important things.

Microsoft's denial is based on its own definition of spyware:

"Broadly speaking, spyware is deceptive software that is installed on a user's computer without the user's consent and has some malicious purpose. WGA is installed with the consent of the user and seeks only to notify the user if a proper license is not in place. WGA is not spyware."

This is patently absurd. Many spyware programs, such as peer-to-peer file sharing applications, are knowingly installed with the user's consent. The user downloads the software to get music, a screen saver, or whatever other benefit is promised.

What makes a program spyware, among other things, is that it operates in ways that aren't clearly disclosed before installation and it reports data back to a central server. Furthermore, this activity needn't be malicious. Many spyware programs do nothing more than serving up targeted advertising or tracking anonymous marketing behavior. If a user wants such tracking functions, they might be fine. But if the user wasn't clearly made aware of this, whether or not such software has a malicious purpose, it's still spyware.

The majority of published definitions of spyware focus the fact on that a program quietly gathers and transmits data. For example, here's an excerpt from the first definition returned by Google when define spyware is entered:

"Any software that covertly gathers user information through the user's Internet connection without his or her

Re: Windows Genuine Advantage – Big Brother is watching you

knowledge, usually for advertising purposes."

To help you understand the latest revelations about Windows Genuine Advantage's behaviors, let's walk through the latest facts that have been discovered about WGA.

What Genuine Advantage actually does:

What we've found about WGA fits neatly into four behaviors that are typical of all spyware:

1. Lack of disclosure before installation. Windows users in the affected countries (U.S., U.K., Australia, etc.) who had Automatic Updates set to "auto-install" received WGA without user action, as though it was a critical security update which it clearly was not. Even those users who ran Windows Update or Microsoft Update manually, however, were misinformed about what WGA would do. In 17 pages of screen shots, ZDNet blogger David Berlind demonstrates this, concluding:

"I was not asked for consent when the WGA Validation Tool the one that, like spyware, phones home installed itself. In fact, as can be seen from this screenshot which immediately preceded the automatic download and installation of the WGA Validation Tool, I could easily argue that I was misled into thinking I was going to download and install something else when in fact, I was downloading and installing, without my consent, software that apparently phones home."

A separate WGA Notification Tool is also downloaded. This program does not contact Microsoft's server, but merely displays warnings on a user's PC if a Genuine Advantage test is failed for whatever reason. After clicking several links in the manual download process, Berlind found only a vague explanation of WGA through what he calls a "circuitous route."

2. Transmits data to a central computer. The WGA Validation Tool contacts a Microsoft server every time a PC is booted up and every 24 hours after that. (Some of the earliest alarms about this were sounded by Lauren Weinstein, a co-founder of People for Internet Responsibility, in postings June 5 through 13.) WGA's "phone home" events, like all Internet packets, contain the IP address of the affected PC and the date and time, indicating when it booted up or had run for 24 hours. In addition, Microsoft's WGA director, David Lazar, told the Associated Press in a June 7 interview that the program also:

"...gathers information such as the computer's manufacturer and the language and locale it is set for." This is enough data to easily identify individual PCs. And, of course, WGA can be modified remotely to collect additional information (as explained in point 3).

3. Downloads other software and morphs itself. WGA's daily contact with Microsoft's servers is specifically designed to allow the company to download new instructions. According to Microsoft's June 8 statement and Lazar's interview, this includes:

- " Changing how often WGA contacts Microsoft's servers;
- " Disabling features of WGA or disabling the WGA software entirely;
- " Adding to the license keys that WGA treats as invalid; etc.

4. Cannot easily be uninstalled. No entry appears in the Add/Remove Software control panel for patches 892130 or 905474 the Validation Tool and the Notification Tool. If you manually delete WGA's executable file, Windows regenerates it. (I'll discuss remedies for this below.)

Re: Windows Genuine Advantage – Big Brother is watching you

Perhaps most shocking is a trait of WGA that most other spyware doesn't suffer from. WGA is beta software that even Microsoft doesn't consider ready for release.

Section 4 of the WGA Validation Tool EULA (End User License Agreement) states:

"4. PRE-RELEASE SOFTWARE. This software is a pre-release version. It may not work the way a final version of the software will. We may change it for the final, commercial version. We also may not release a commercial version."

Microsoft's June 8 statement confirms this by repeatedly calling the WGA rollout a "pilot program" or a "pilot version." Of course, "pre-release software" and "pilot version" mean exactly the same thing – beta.

At least that explains some of the many problems that Windows users are having with WGA.

Problems with WGA and some solutions:

It's important to remember that Windows Genuine Advantage is not an omnipotent, do-everything program. Its stated goals are simple. If an instance of Windows doesn't seem to have a valid license, (1) display notices to the user and (2) prevent any updates being downloaded from Microsoft.com except security upgrades that are rated "Critical."

Despite these limited tasks, WGA seems to cause a wide variety of headaches. Since my May 25 article appeared, I've collected reports from the field and from readers describing the following categories of issues:

1. False positives of legitimate copies of Windows. Numerous users report that WGA refuses to validate licensed copies of Windows that are unquestionably genuine. At Microsoft's official online forum called WGA Validation Problems, many people report problems even with packaged copies of Windows that were purchased directly from Microsoft.

2. No updates at all unless WGA is accepted. Although a WGA failure is supposed to only prevent affected users from downloading nonsecurity updates, many Windows Secrets readers report that legitimate copies of Windows refuse to display any updates except the WGA download until the Validation and Notification Tools are installed. Phillip "Skip" Lehrfeld writes:

"I chose to download the Windows Genuine Advantage Validation Tool (KB 892130) on March 6, 2006. I followed this with Windows Genuine Advantage Notification (KB 905474) on May 4, 2006.

"On June 2, 2006, I was checking the Update site as I was informed that there was a new Critical update to be downloaded. I checked the site and it told me I could not get my update as I was missing a critical tool. I checked it out and it told me I was missing the Windows Genuine Advantage Validation Tool. I checked my history and sure enough I had installed it on March 6.

Re: Windows Genuine Advantage – Big Brother is watching you

"OK, I will bite, and I downloaded it again. Yes, the number was KB 892130, the same as before. Then it wanted me to install the second one again. I installed Windows Genuine Advantage Notification, KB 905474, for the second time. Having installed the two for the second time, there were no new updates to install. Those were the updates to be installed. ...

"After the reinstallation, I checked the history section of the site and now I have the two updates installed twice successfully.

"I have an authorized copy of Windows XP and had no problems with the above events; but it leaves me to wonder what is going on and are they now doing something else to my system without revealing what is going on."

The redundant WGA install messages are probably caused by changed code that Microsoft wished to download to defeat some workarounds that disabled WGA.

Numerous other readers say that Microsoft's update site also reported to them that there were no patches except WGA, although important updates were, in fact, available.

3. "Notify only" options disabled. We have some reports that the "notify only" options in Automatic Updates are greyed out and can't be selected. G. Allen Taylor, M.D., writes:

"With regard to the OS updates, which I have so faithfully and obediently installed, I now suspect that one of them has 'grayed out' the Options menu in Windows Update on both my computers. "While formerly I could choose to automatically or manually download and/or install the periodic updates, I now have no choice on either of my computers. Whether I want them or not, all updates are downloaded when I'm online and installed then or the next time I reboot."

Dr. Taylor offers a fix, which involves the fact that a Group Policy was somehow enabled that prevents any option other than auto-updates.

The solution requires a change to Group Policy or the Registry. The procedures are described at the Windows XP MVPs site.

4. Reinstalls from valid CDs fail the Genuine Advantage test. By far the most serious side-effect of WGA is that it doesn't validate instances of Windows that are reinstalled, even when a genuine CD-ROM from a major computer maker is used. Lauren Weinstein writes:

"It appears that it is exceedingly common for repair operations to reinstall based on "cloned" or otherwise duplicated copies of the Microsoft OS, rather than try to restore or reauthenticate based on the original users' OS serial numbers or authentication codes. Original restore disks and key information cards/labels are frequently missing, making it difficult to duplicate the original authentication environment."

I've seen reports of this on Microsoft's own forum involving such cases as Best Buy's Geek Squad reinstalling Windows with the user's original, licensed Dell CD-ROM.

Despite all of the reported problems, Microsoft officials aren't very forthcoming on the subject of WGA. On June 9, I asked to interview David Lazar in Redmond and submitted a few questions in writing. Five days later, a spokesman replied, "Unfortunately, we will not be able to participate in this opportunity."

Many Windows users seem to be in denial that WGA could be spyware, because Microsoft is such a big, well-known company. Unfortunately, that was what people thought of the Sony BMG recording label before it started distributing music CDs last year with rootkit software that infected PCs.

Re: Windows Genuine Advantage – Big Brother is watching you

I don't feel that Microsoft or Sony BMG are evil incarnate. But we must recognize that Microsoft is now just one more spyware distributor among the many we have to watch out for.

--end of quote--

Time for an Apple.

.