SpyWorks is not Spyware
(a non-technical explanation).
by Dan Appleman
President, Desaware Inc.

Let me start by making one thing perfectly clear. I HATE spyware. In my book "Always Use Protection: A Teen's Guide to Safe Computing," I spend a lot of time covering the dangers of spyware and teaching how to remove it.

Some anti-spyware programs mistakenly detect some of our software as spyware. When we find out about it we contact them, and the responsible ones remove our software from their list.

In this article you'll learn the inside story of what is going on, what our software really does, and maybe a bit more about how to protect yourself and not harm your system in the process.

How a Keyboard Logger Works

One of the tricks spyware uses to spy on you once it's on your system is to intercept keystrokes to find out what you're doing and maybe capture user names and passwords. The first thing you need to know is that every keyboard logger uses a feature that is built into Windows called a "keyboard hook."

That's right – keyboard hooks are built into every Windows system. The feature is part of a file called user32.dll that is typically found in your windows\system or windows\system32 directory. DON'T DELETE THIS FILE! If you delete it, you'll destroy your Windows installation – it's one of the main parts of Windows.

You may wonder: why did they build that feature into Windows? Well, there are lots of useful things you can do with keyboard hooks:

- You can create hot-keys, where a keystroke can be used to bring up one application while working on another.
- You can build a keystroke "macro" recorder that memorizes tasks so they can be easily repeated.
- You can build "smart forms," where a program watches as you type and guesses what you will type next, speeding data entry.

There are a variety of other features that a program can use keyboard hooks for that make a program work better, none of which pose any problem or security risk.

Unfortunately, Windows has no way of knowing whether a program using a keyboard hook is harmless or dangerous spyware.

Where does SpyWorks come in?

Programmers use a variety of computer languages to write programs. Many use a language called C++. C++ programmers can use keyboard hooks by simply telling

Windows that they want their program to see every keystroke on the system. It's easy – just takes a few lines of code.
Another popular programming language is Visual Basic (VB). Visual Basic programmers have traditionally had a harder time communicating with Windows. There were many features in Windows that were difficult for them to use, including keyboard hooks.
SpyWorks is a set of software components – files with extension .OCX and .DLL – that allows VB to communicate more easily with Windows. The components perform a wide variety of tasks – they allow programmers to customize the look of Windows, to detect when you move the wheel on your mouse, to add pictures to menus, and add many more features to their programs to make them look and work better, and make them easier for you to use.
All of these features are made possible by making it easier for VB programmers to communicate with Windows. In fact, the entire purpose of SpyWorks is to allow VB programmers to do the same kinds of things that C++ programmers can do.
This is the key thing to remember: The SpyWorks components themselves do NOTHING on their own. They are just a go between – allowing VB programmers to do the exact same things that C++ programmers can do – using capabilities already built into Windows.
Most programs that use the SpyWorks components use those capabilities to perform their normal tasks.
Unfortunately, it is possible for someone to write a spyware program in VB using SpyWorks components to access those built-in Windows capabilities to perform its malicious task.

What to do about spyware?

Remember, the SpyWorks components are just go betweens – an intermediary between a VB program and Windows. In those cases where a spyware program is written in C++, there is no go-between, so the trick to removing the program is to find it and erase it. That's what anti-spyware programs try to do. But in those rare cases where a spyware program is written in VB, the trick is to remove the program without removing the SpyWorks components. Why wouldn't you want to remove the SpyWorks components? Because other programs might require them for their normal operation. Removing those components would be like removing user32.dll – in that case removing the keyboard hook functionality of Windows destroys Windows. In this case removing one of the SpyWorks components may destroy other programs as well.
Unfortunately some anti-spyware vendors are lazy – they think that just because a program uses SpyWorks as a go between, SpyWorks is also malicious. That's simply not the case.

A more detailed example:

Imagine a hypothetical spyware program. This program might intercept every keystroke, store it in a file, and send it through Email to some email address.
Such a program might use SpyWorks to tell Windows to place the keyboard hook. However, the SpyWorks component itself only passes keystrokes between Windows and the program (it's the go-between). The component doesn't do anything with the

keystrokes. It can't save them to disk. It can't email them. It has no Internet capability at all.
SpyWorks itself is no more spyware than Windows is.

How did the SpyWorks components get on my system?

Every now and then we get a call from someone who discovered one of the SpyWorks components (dwshk32.ocx, dwshk36.ocx, dwspy32.dll or dwspy36.dll) and wonders how they got on their system.
Remember how earlier in this article I wrote that VB programmers use the SpyWorks components to perform a variety of tasks? Well, there are actually many companies that create software components that can be used by programmers to create applications. Those components can do many different things, from generating reports, to accessing the Internet, to creating nice graphical buttons or menus.
When you install one of these programs, the installation process must also install all of the components that are used by that program. Some of those components will be installed in the installation directory, but others are typically installed in the System directory. That's because most of these components can actually be shared by many different programs and need to be in a location where they can be found by all the programs.
So it turns out that these files got on your system because you installed an application that uses them. That's why it's important you don't just go removing them – doing so might break a program you're using. If you do want to disable them for some reason, it's better to just rename them. Then you can try your other programs and see if any of them stop working properly.

SpyWorks – A suspicious sounding name

The SpyWorks product was created long before the Internet became popular. In fact, the original version was distributed on floppy disk because even CD-ROM drives were few and far between. Almost nobody had Internet access. We were still using slow modems to dial into local bulletin board (BBS) systems. Computer viruses existed, but were spread by infected floppy disks. Nobody had heard of spyware.
We named it SpyWorks because of a term that was common among Windows programmers at the time. Microsoft had a program called Spy that would display windows messages – a way to find out what Windows was doing and how it was controlling and interacting with a program. Since our components allowed VB programmers to use Windows messages (another thing that normally only C++ programmers could do), we named the product SpyWorks. Had we known at the time that someday spyware would be such a problem, you better believe that we would have chosen a different name!