Association of Shareware Professionals, Inc

Membership:
www.asp-shareware.org

Consumers:
www.asp-shareware.com

Spyware: Consumer's Guide

What Software Users Need to Know

by Jerry Stern
Editor, ASPects
Newsletter of the Association of Shareware Professionals

First, there's no such thing as spyware. The publishers of spyware would certainly know, and there aren't any publishers who identify their product as spyware, so it doesn't exist. That's proof, right? Yeah, right.

No, really. The publishers of software that provides targeted advertising based on your web surfing have announced publicly that their products are providing a positive service. Their programs provide a service, possibly a $30 coupon on office supplies when you visit an office supply site, or a program that alerts you to weather changes from the system tray of your computer, or adds smiley faces to your email, or adds background pictures to the menu bars of your web browser, or maybe a free screen saver.

Forget for the moment that the $30 coupon is for a competing office supply site that has chosen to do business on the basis of displaying ads based on the use of a competitor's registered trademark, and that the ad may pop up as a disruption at any step of the sales transaction. Forget the concepts of restraint of trade and improper use of trademarks. Forget as well that screen savers do nothing to save modern monitors–they're only for entertainment for when you are NOT actually looking at your monitor.

The publishers of such products call them adware, and assure us that no personal information is being transmitted, including no information identifying web sites that you've already visited. That, of course, leaves as a total mystery how the software can request a specific ad be sent to a specific internet connection without identifying the ad that's needed. Must be magic.

No, the point is that these companies provide a value, they say, and that their customers have all accepted the license terms of the agreements, yes, even including this gem:

To the maximum extent permitted by law, in no event will COMPANY *or its agents be liable for any damages arising from the use of or inability to use the software, including, without limitation, damages to users' systems and/or software and/or data, computer failure or malfunction, computer virus transmission, performance delays or communication failures, security breaches or any and all other damages or losses...*

Or here's another sample: *The Software and the Service is in a pre-release beta state only and may contain errors or inaccuracies that could cause failures, loss of data, and/or conflicts or problems resulting from the use and/or operation* *of other software installed on your computer or which you may wish to install in the future, whether used separately or in conjunction with the Software.* COMPANY *does not guarantee or assume responsibility for any of the foregoing or any other consequence of using the product. Licensee agrees that due to the experimental nature of the Software and the Service as a beta product, the Licensee will not rely on the Software or the Service for any reason and has decided to download and use the Software and Service at his or her own risk.*

OK, so these programs are admittedly unstable. Combine two or more of them on one computer, and there will be conflicts, errors, and inaccuracies. In English: your computer will slow down while the software programs battle in the background for control of the processor, the browser, and the internet connection. The more of these products you have on your computer, the worse things get.

By using the Internet and/or the Software and/or the Service and/or the Content, Licensee may be exposed to contaminated files, computer viruses, eavesdropping, harassment, electronic trespassing, hacking and other harmful acts or consequences that might lead to unauthorized invasion of privacy, loss of data and other damages.

Now that's a great model for publishing software. Basically, you can have one of these programs running, and not more, before interference begins with your computer. It doesn't actually matter if you are using the free weather reports at a different time than the free screen saver; they are both sitting in computer memory all the time, and competing for cpu time, much like a large group of 2-year old children.

You agree to indemnify, hold harmless and defend COMPANY *and its subsidiaries, affiliates, officers, agents, co-branders or other partners, and employees, at your expense, against any and all third party claims or demands, actions, proceedings and suits and all related liabilities, damages, settlements, penalties, fines costs and expenses (including, without limitation, reasonable attorney's fees and other dispute resolution expenses) incurred by company...*

There's another goodie, and this one is from a point-to-point file sharing program that may, at its discretion, choose to use your computer to index the contents of other computers. You pay the legal expenses of the publisher of the product.

So, are any of these products spyware? Maybe. As of the Spring of 2004, the working definition of spyware for the Federal Trade Commission and the U.S. Congress, is *“software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge.”*

These products are spyware, then, IF you choose to define “the consumer's knowledge” to not include information in a license agreement that does not display on-screen during the installation. None of the snippets of legalese above is visible without either following links back to a publisher's web site, or scrolling down through multiple pages of contract-talk in a small screen box that displays only the first few lines of the document. Most consumers have been conditioned to skim past such license agreements, thinking that they say the usual–that the publisher provides no warranties beyond the price of the product, and that the end-user is not allowed to give away the product to anyone else, or try to take it apart and so “reverse-engineer” it. Such statements from shelfware products are many pages long, and include such tidbits as declarations that a desktop operating system may contain components that are not suitable for running critical life-support equipment. No, I can't make this stuff up–truth, as written by lawyers, is bizarre without my help.

Problems

Well, I've ranted long enough about what spyware is not. Let's get on to the practical information. First, spyware and adware, at a practical level, only differ in one way. All adware, and most spyware, with the exception of some programs that exist only to steal information for non-advertising reasons, use your computer for showing you extra advertising, above the level that you would normally see during web surfing. Both run all the time that your computer is on. Both steal computer speed and internet bandwidth. But spyware sends information home, and adware may or may not send personally-identifiable information. Overall, both are leeches on your computer that can damage your software installations and convert a fast computer into a doorstop. Treat them as one problem.

A big infection of spy/adware is expensive to clean up. As a system technician, I do these cleanups regularly, and the bill is never less than $160, averages around $220, and has gone as high as $480. That's for two to six hours of work, at on-site consultant rates of $80/hour, which is mid-range for computer consulting work nowadays. And a cleanup may not result in a complete fix–sometimes settings for other programs are lost, along with shortcuts, favorites settings, emails, and possibly business data. I won't pretend to put a dollar value on business data that is remotely copied by spyware or that is wiped out entirely when multiple spyware programs cause enough system disruption to start damaging the computer's file allocation tables. That's the FAT, for short–think of it as the index to your file cabinet.

Prevention

Spyware and adware gets onto your computer in two basic ways. First, you see an offer for software that sounds good, and you install it, probably without reading the license agreement that tells you what it may do in the background. You prevent these by being suspicious of free products that appear to have no way of making money.

Second, there's the drive-by download. That can happen when you visit a web site that contains programming code to automatically run software on your computer. That's supposed to be impossible, but all browser software has security holes in it, and most computer users don't patch the holes.

What happens is that someone finds a security hole in a browser. That person usually posts a notice that they've found a way to “execute arbitrary code.” If they're responsible researchers, that information is sent to the publisher of the software. If the person or group that found the gap isn't quite so much concerned with security as with other issues, they may publish the information in private or public newsgroups for hackers to play with. From there, it's something of a race to see whether the software publisher can release a patch and get it installed before the hackers find an “exploit” for the hole, which will use the security hole to do something unexpected.

Usually, by the time an exploit virus or worm or drive-by download surfaces for a particular hole, a patch already exists, and only users who haven't been updating their browser and operating system software will have problems. Sometimes, the exploit will follow the patch by 6 months, or a few weeks. And sometimes, the exploit will happen before a patch exists, so having all the patches in place is important, but it does not prevent all problems.

Scanning for Routine Cleanups

Good prevention includes using more than one adware scanner regularly. One is no longer enough, because each adware scanning program has its own list of bad stuff, and may not clean out everything, and because some spyware and adware are self-repairing, and will detect and stop or damage some scanning software. As a starting point, choose two anti-spyware programs based on recommendations from trusted sources, scan weekly (more often if you find more than just cookie files), and clean out everything suggested for deletion.

Be aware that there are some spyware scanners that are themselves spyware. That's why you want to read reviews and ask for recommendations on cleanup programs. Also note that some of the removal programs run in cleanup mode only, or can also run all the time in the background, much like an antivirus program, and prevent infections. Sounds good, but that's going to cause problems for many users as the antivirus program publishers start adding most spyware to their bad-guy lists for removal. It's not a good idea to have multiple programs scanning software at the same time–such a cure for spyware is nearly as bad as having multiple adware programs running–system speed suffers, and doorstop-syndrome can set in.

Backing up your Data and Computer

In the worst case scenario, a major spyware/adware infection is going to be as bad as a virus infection. There's nothing worse, short of the computer being stolen. So back up your data constantly, and backup the entire hard drive on a regular schedule, using a product that creates an “image” of the entire hard drive, and that can restore the drive completely from a boot disk and backup set of CDs or DVDs, when needed. And store those backups far away from the computer (several miles is good) so that the backup is good against all types of generic disaster.

Get Help for Big Cleanups

If you have proper backups, you should never need professional help to clean up a computer after a virus, spyware, or adware infection. But most users don't back up their computers, don't install browser patches, and don't run up-to-date antivirus software, so when the time comes that you need help, it's best to get a referral from someone local who knows a tech or consultant that works with cleanups regularly. While hiring the computer genius 10-year-old from next door may be a great way to trouble-shoot a game program, nearly the best choice is to work with a full-time professional when doing a system cleanup. The very best choice is to prevent the whole issue by following a few basic guidelines:

First, always ask why software is free, and what the revenue model is for a big free program. It's rarely paid for by giving it away in volume. Choose software from companies that provide support, return messages, and offer warranties, and that make their money by actually selling software.

Second, protect your computer by not running any software that shares file across the internet. These are called peer-sharing programs, used mostly for music and video sharing, and they leave your computer wide-open to attack, and are a very large part of the spyware program.

Third, check for and download browser patches and virus updates on a regular schedule. Automate the process–it's very easy, compared to having to cleanup the mess later on.

Fourth, run scheduled scans for spyware, adware, and viruses.

Finally, back up everything. And then back it up again, and store the backups far away from the computer.

As a computer user, the difference between spyware and adware is whether or not you believe a claim that your personal information has been transmitted. It's a good-faith question based on trusting companies that use your computer and internet connection as they see fit. While some adware companies might be honest, you have no way to know, so treat spyware and adware as the same problem, and don't let them take control. Backup and patch regularly, install software only from trusted sources, and always think before you click.

Jerry Stern is the editor of ASPects–the monthly newsletter of the Association of Shareware Professionals, and is the author of Graphcat and FileTiger, runs Science Translations Software, and is online at www.filetiger.com

The ASP is a not-for-profit association of over 1,000 independent software developers, marketers and vendors, most of whom use the try-before-you-buy method of software distribution and marketing. For more information on the ASP, visit our consumer information web site at www.asp-shareware.com.