Spyware, Adware, Malware, Thief

Creating Business Income from Denial of Service and Fraud

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

Labels blur and change with time. It's behavior that's important, and not the common label for it. That makes legal approaches to stopping harmful actions difficult. If your definition of an act that could be made illegal is imprecise, the behavior continues, and law-abiding citizens are restricted from activities that are beneficial to consumers and the economy.

For software, the labels have changed quickly. Good labels have become bad words. Marketing methods that worked well in the 1990's have been taken over by con artists in these opening years of the new century.

I've been watching the industry from the inside for years now. I've been publishing software since 1984, writing about computers and software since 1988, marketing shareware since 1991, and have been helping local clients keep their computers working for the past decade. For the past two years, that has meant sudden increases every few months in virus removal, adware removal, spyware removal, and removal of phone-home components from boxed software and hardware products that slow computers down to the point of being doorstops.

Since personal computers became available in the late 1970's, software has evolved from very expensive to inexpensive, and sometimes free. Back then, small programs developed by an independent programmer were frequently given away. A few innovative programmers started to ask for contributions to help finance additional development of larger programs such as PCWrite and PC-File , and shareware marketing of software began. There were other such software labels in those days, including postcardware, begware, bannerware, freeware, and dozens of others. In 1987, the Association of Shareware Professionals was founded in order to promote the creation of try-before-you-buy software, or shareware.

Now, shareware is commercial software, sold mostly online, marketed with downloads of try-before-you-buy editions of the product. It's the same approach as the free sample of a product in a grocery store, and while there are many variations on how the shareware edition sells a full commercial software product, the successful authors all have this in common: the shareware experience has to get a customer interested in the product and happy with the free trial so that money will be spent on the full version software. Shareware authors cannot anger customers with autostart changes and

other surprises and still expect payment. Most other approaches to making money with software aren't that easy to categorize.

Definitions of these other types of software are far more difficult. Adware is a good example. Adware was a good thing, at one time. In 1992, adware was software given away for free that included an advertisement for other products sold by the same author. There was no connection to the Internet to get ads–this was before the WWW explosion, and the advertisements were just a handful of graphics or a few paragraphs of text that were included with the software.

By 1998, adware's definition had changed. It became a free product that downloaded advertisements through an internet connection from a third-party ad agency, displayed the ads in the same window as the program, paid the author on the basis of how many ads were displayed, and the ads never appeared by themselves. Most authors found that adware, as it existed then, didn't pay well enough to support additional program development.

2000 was when things changed. Venture capital entered adware, in a big way. Within the shareware industry, authors saw big money devoted to drawing products and authors away from the free download of a try-before-you-buy product, attempting to convince authors that being paid a few cents for every download of a product with advertising sponsors was more profitable as a marketing model than being paid $30 for a product license. At the industry convention that year, authors were told by one startup exhibitor that they could earn a $17,500 bonus for incorporating a new component into their products and offering them for free download. That component would add a text-only advertisement in the title bar of Internet Explorer, running anytime that Internet Explorer was running, whether the free product was running or not. That was the turning point, when the advertisements were no longer linked to the free software. That particular experiment didn't do much; a good time was had by all at the party and casino night, but only a handful of authors signed up, and the venture company had disappeared by the following Summer.

Since then, adware has become a bad word, linked to spyware and privacy violations by everyone except the publishers of the products. Now, adware shows up as free software that will put a convenient tool in your taskbar to do a task for you, possibly storing passwords, putting smiley faces in email, or weather reports on the desktop, or as a free screen-saver of the month. Adware and spyware are particularly prevalent in software products that are themselves illegal or potentially so, in particular software for file sharing and copying music and movies. The majority of adware is installed on the basis of stealth, hiding what it does in a license agreement on a web site, subject to change at any time, without notice, stating that the software item "collects and stores information about the pages you view" and "may use that information to provide targeted ads." But most don't mention that they work full-time, and that installation of more than one of these software gadgets in combination can turn a fast computer into a blithering slowpoke.

Worse, much spyware/adware is installed on the basis of a popup message, along the lines of "Would you like to not continue installing (gadget name), and give up (feature)?" Many computer users automatically think they've read the message that a program wants to install a graphics viewer add-in, and immediately click 'No.' Wrong answer–that meant 'install.' This is deception at best, and in many cases, fraud.

So, why was adware a good thing ten or fifteen years ago, and bad now? Well, compare it to television commercials. Some commercials are annoying, some are funny, some are just too loud, but all of them go away when you

change channels or decide you'll play a movie from DVD instead. That was adware in the early days–it paid for the program it came with, it said so up-front with no trickery, and if you didn't use the program, or uninstalled it, the ads went away.

Adware as it exists now, to continue the television comparison, would be something like this: "In exchange for watching the program (name here) you agree that your television will show ads of our choice, which may be adult or deceptive in nature, at all times that the television is turned on, and may interrupt other programming to do so at our convenience, and may tie up your phone line to get more ads and send home information about your viewing habits." Well, it's my computer, and my television. If a company wants to give me a free television or a free computer, I'll take it for whatever value it provides, and keep it and tolerate the advertising as a cost of having it available, or choose not to take it. But that's not adware as it exists now. It's my computer, not theirs.

The lines for adware are even being blended into virus and trojan territory. Clearly, much spyware is a trojan–it's the gift horse with the phone-home software inside. But some virus-writer's techniques are finding their way into adware, and denial-of-service attacks have come to mean both a virus that floods a web site with data to prevent its use, and a spyware program that slows down a single computer while it phones home for more ads, and to act as a server for advertising on other computers.

As I've removed these little monsters and thieves of personal data, I've found that many are self-repairing, just like the newer viruses and other malware. Remove one autoplay entry for some of these products, restart the computer, and it will come right back. There are multiple starting points, all checking for and repairing each other, so that professional cleanup tools are needed to root out all the infected parts of the software at once. Cleanup of adware or spyware isn't much different from cleanup of a virus or worm.

So, is boxed software or the software that accompanies hardware any better? Usually, but not always. Some boxed software, or shelfware, connects to a server back at the publisher for a variety of purposes. Some do it for a valid reason, such as product updates. Some will phone home for license validation, and while that's a touchy subject for some consumers, as long as the publishers announce what they're doing, and why, before purchase of the product, and don't send private information home without permission, it's a valid choice for how to compete, make a profit, and use that profit to continue supporting and developing the product.

Some boxed software, however, doesn't play fair. For example, a major manufacturer of color photo printers installs, along with their drivers for printing, a series of four extra programs that automatically run when Windows starts. Surprisingly, at least to most owners of the printers, disabling all four of those programs does not result in any loss of printing functionality whatsoever. What those programs do isn't documented, but judging from filenames, apparently at least one is intended to assist users in publishing photographs onto a web site for an additional fee. It's a stealth install; no permission is asked, but it's there, and it slows some computers down markedly, and reduces stability, and costs productivity.

Labels don't seem to matter much. Adware and spyware are imprecise descriptions of what these programs are doing. We can't prohibit anything on the basis of labels; publishers will just say that they're something else, and make a

small adjustment in their products to match the new definition. It's behavior that must be banned.

What behavior cannot be allowed, then? First, all unannounced installation of a software component that will autostart when a computer is turned on should be prevented by legal prohibition, and by intervention from the operating system. If the operating system could pop up a warning of "An installation program is attempting to add a program to the autostart list. Allow yes/no?", much of the adware would simply go away.

Next, all unannounced use of an internet connection should be prevented, again both legally and by intervention by software. The software part is possible now, using software firewalls.

Finally, stealth installations have to be both banned and prevented by software. Clicking on a program to "view weather" should not do anything other than "view weather."

While law and technology attempt to catch up with the adware publishers and the virus writers they've hired, what can consumers do? Unfortunately, the answer is to watch what they're clicking on carefully, backup their computers, and run scans for adware just as they run scans for viruses and other malware.

Further, when software is offered for free, consumers have to ask two questions: First, why is it free? If the answer is that "It was a project I created in a day for our own use, and I'll donate its use to the public (no support calls, please) for their own use," and if you trust that statement to be true, great. And there is a lot of such free software out there, especially in the open source community, including applications for Linux. Or if the answer is "I no longer support this product, but it's available for those who still need it" OK, then as a user of free software, you know what you're getting, and that's the key.

The second question to ask of free software is "What's paying for this? What's the revenue model? Is there any visible way that the free software is providing income to this software publisher?" A free try-before-you-buy download of a shareware program is advertising for purchasing the program itself, and that's OK. Or built-in advertising can pay for free software, and you'll want to know that before installing the program.

Some products don't need revenue, if they're small programs that don't need support or updates, or written by a community of authors. But if the publisher is putting major advertising efforts into getting you to download free software with no visible means of support, there's something wrong, and being a careful and suspicious consumer is just as important for a downloader of software as it is for someone selecting any other consumer product.

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.
