

## **Comments by Eric L. Howes on the Problem of Spyware in Advance of the FTC April 2004 Spyware Workshop**

Mar. 29, 2004

Federal Trade Commission  
Office of the Secretary  
Room 159-H  
600 Pennsylvania Avenue N.W.  
Washington, D.C. 20580

Re: Spyware Workshop – Comment, P044509

The FTC is to be commended for hosting a workshop on the problems that spyware poses to consumers and citizens on the internet. Spyware is fast becoming the most serious threat to the privacy and security of internet users, and it is imperative that the FTC take action to protect consumers and citizens from the unscrupulous behavior of companies that use advertising software to force their commercial messages on unwilling and vulnerable consumers. These comments are submitted with the hope that they might aid the FTC's efforts to understand the threat of spyware to consumers and develop an effective response to it.

### **Background**

I am a graduate student in the Graduate School of Library and Information Science at the University of Illinois at Urbana-Champaign. For the past twelve years I have also taught business and technical writing at the University of Illinois. More recently I have begun teaching at Parkland Community College in Champaign.

Over the past four years I have maintained a personal web site at the University of Illinois (<http://www.staff.uiuc.edu/~ehowes/>) to supply internet users with resources to protect their privacy and security on the internet. Among those resources are several utilities and "block lists" that allow users of Microsoft's Internet Explorer web browser to protect themselves against the flood of unwanted software and content pushed on them by aggressive advertising and marketing entities.

In recognition of my work to help internet users protect their privacy and security, Microsoft recently awarded me its MVP (Most Valued Professional) Award (<http://mvp.support.microsoft.com/>).

### **Experiences with Spyware**

My experience with spyware stems not only from the time I spend helping users troubleshoot PC problems but also from the research I perform to update the tools and "block lists" used by visitors to my web site. Users, including my students, frequently ask me for help removing spyware from their computers, and I provide advice and support both online and in person. In addition to assisting users, I have also spent thousands of hours in online forums over the past few years, examining HijackThis! logs posted by users with spyware-infested systems and investigating the software and companies responsible for the problems of those users.

In working with students and online users, I have watched spyware grow from a marginal problem that once affected only a small number of users who unwittingly installed advertising supported freeware (often called "adware") to a commercial plague of aggressive "hijackware" that now afflicts the majority

of the PCs of users who request help from me. During the few years that I have researched spyware for my "block lists" and other tools, the number of web sites known to distribute aggressive "hijackware" has grown from a few dozen to a few thousand; the number of companies or entities engaged in distributing spyware has grown equally fast. Most alarming to me, though, is the increasingly aggressive nature of this spyware, whose creators seem to find ever more sophisticated ways to push their software on unsuspecting users and hijack consumers' computers for commercial purposes.

The spyware that I find installed on users' PCs proves troublesome to users for three reasons. First, users who request help are simply bewildered and flummoxed by this spyware. They almost never know how it was installed on their computers and do not recall ever having agreed to the installation of such software. On the rare occasions they do remember the installation, users maintain that they did not fully understand the true functionality of the software. In many cases these users do not even recognize that spyware is installed on their computers and mistakenly attribute their PCs' problems to more traditional (and familiar) "malware" such as viruses, trojans, and worms.

Second, these spyware programs can severely degrade the stability and usability of victims' PCs and prevent consumers from using their computers and internet connections as they choose. The computers that I fix are usually sluggish and unstable, prone to errors and crashes, and are unable to connect to the internet in some cases. Even when the performance of their PCs is not degraded, these spyware victims are frequently subjected to a raft of unwelcome system changes. Users often complain that their desktops are littered with intrusive pop-up advertising, that unwanted toolbars and other widgets have been added to their browsers and desktops, and that their browsers' default home page and search engine preferences have been changed without their consent.

Third, however, these users often cannot remove the spyware from their PCs by themselves or even prevent the future installation of unwanted spyware. The vast majority of users that I help are not "computer savvy" and find even basic computer maintenance tasks challenging and intimidating. These people are typically not aware that some spyware can be removed with an uninstaller provided by the vendor. In cases where an uninstaller is not available or fails to do the job, these users face significant hurdles in attempting to use an anti-spyware application to remove the unwanted software. When these users do manage to locate and download effective anti-spyware programs, they often cannot use those anti-spyware programs properly and effectively because the problems that the anti-spyware programs identify on their computers are simply too numerous and bewildering. Still worse, spyware victims are usually unfamiliar with what they could do to prevent spyware from being installed on their computers in the future, and the preventative solutions that do exist frequently prove too complex and frustrating for these users to employ.

## **A Typical Case of Spyware**

The most recent case in which I fixed a student's computer is a good illustration of the problems I have just summarized. One of my students came to me because her PC (less than a year old) had suddenly stopped connecting to the internet, preventing her from accessing her email, browsing the web, or using her instant messaging software. This broken internet connection proved especially troublesome because she was in the middle of a job search, and had been researching and talking with companies online in order to secure employment after graduation (just a few months away). As I questioned this student about her PC's behavior, she complained about a number of other problems including system instability, inexplicable error messages, and the mysterious appearance of pop-up advertising on her desktop. She thought her PC's problems were caused by a virus or worm of some sort.

When I finally sat down at her computer the true cause of her PC's problems became clear. Her computer was not infected with a virus or worm (a system scan with a reputable anti-virus program confirmed as much). Rather, a dozen or so different varieties of spyware were installed and running on her computer. One of those spyware programs I immediately recognized because it replaces key Windows networking files and reconfigures systems' networking settings -- a likely cause of her broken internet connection.

To remove the spyware, I first ran every vendor-supplied uninstaller that I could find. Many of the spyware programs had not shipped with an uninstaller, however. While some of the associated companies may make uninstallers available on their web sites, we could not access those web sites because the PC's internet connection was broken. Still worse, the uninstallers I did manage to find failed to remove the associated spyware programs completely. More importantly, though, even after I had run the vendor-supplied uninstallers the PC's internet connection was still broken.

This student had managed to download and install SpyBot Search & Destroy 1.2 a few days earlier (I had recommended that anti-spyware application to her class). She had failed, however, to update the program's definition databases (she didn't understand that it was necessary to do so). Moreover, she hadn't fixed any of her PC's problems because she found the long list of problems that SpyBot reported too daunting and confusing. And no wonder: when I ran SpyBot Search & Destroy, it flagged several hundred serious problems to be fixed on her PC, and that was with severely outdated definitions.

After I ran SpyBot Search & Destroy and rebooted the computer, SpyBot did manage to fix the vast majority of the PC's problems, some of which had been left behind by the vendor-supplied uninstallers. SpyBot even restored the PC's internet connection, which the vendor-supplied uninstallers had failed to do. With the internet connection restored, I then downloaded Ad-aware 6.0, new definitions for SpyBot Search & Destroy, and several programs to protect her computer from future spyware. I had to perform several more system scans with SpyBot and Ad-aware before this student's computer was finally usable. Before leaving, I installed several programs to protect her computer against future installations of spyware, though she had difficulty understanding how those programs work.

This student's encounter with spyware is all too representative of the problems that average internet users report with spyware. As I identified one spyware program after another on her computer, I asked this student if she remembered installing each program or consenting to its installation by clicking through a EULA (end user license agreement). With every single one of those programs, she insisted that she had not knowingly installed it (though she did recognize the name of one of the programs because of the pop-up advertising on her desktop).

When I found the particular program that had broken her internet connection, I even explained that program's ostensible purpose or function and described the company's business model. Not only was she unfamiliar with the program, she was positively bewildered by its functionality (and this, mind you, is a program from a company who insists that users always consent to installation of its software by clicking through a EULA at some point).

All of the spyware programs on this student's computer, I should add, were installed via the web; there were no advertising-sponsored "freeware" programs (such as P2P file sharing applications or "download managers") on her computer -- I checked.

This case of spyware is quite similar to those of most other spyware victims that I have helped online and in person. In working with such users and their PCs I have learned that:

- Spyware is usually installed on victims' computers without their full knowledge, consent, and understanding;

- Spyware is sufficiently complex and confusing that users find it difficult or impossible to keep spyware off their systems;
- Spyware frequently trashes users' computers, denies users the full enjoyment of their PCs and internet connections, and even prevents its victims from fixing the problems it caused;
- Spyware often proves too difficult to remove for normal internet users, even after users download and install anti-spyware applications;

Some spyware victims do manage to get help from more experienced users, either through an online forum or in person. Those who cannot get free assistance from experienced users, however, might need to call tech support from their OEMs or take their PCs to a computer repair shop and pay for a system repair or re-installation, either of which can prove expensive.

Whether or not they manage to get help, spyware victims are denied the full use of the PCs and internet connections that they purchased. Moreover, they are forced to waste an untold number of frustrating hours repairing the damage to their PCs and restoring their systems to a fully functional state (if indeed they ever manage to do so).

## Ten Myths About Spyware

As consumer outrage over spyware has grown, the spyware industry has developed a number of excuses to defend its software and behavior. Let me address the most frequently propagated excuses or myths about spyware.

### Defining Spyware

*1. Software that doesn't surreptitiously monitor users and collect personally sensitive data is not spyware and thus isn't of any concern.*

Although the term "spyware" has proved popular with internet users, it has caused more than its share of confusion because the term implies functionality (data gathering, backdoor connectivity, etc.) that some intrusive, unwanted software may not have. We should not let a confusion over terminology, however, distract us from the real goal of protecting users from unwanted, abusive software that is installed on consumers' PCs without their full knowledge and consent.

The term "spyware" was first used to describe unwanted commercial software during the spring and summer of 2000, when consumers became aware of "adware" -- advertising sponsored "freeware" -- which often does monitor system use and report potentially sensitive data to advertisers for the purpose of targeted advertising. The term "spyware" proved to be a catchy one, and consumers were soon using it to describe or name all manner of unwanted software that engaged in unwelcome behavior -- even software that did not technically "spy" on users. In other words, the term "spyware" has become a loose, broad term used by consumers for a wide variety of unwanted, intrusive software that consumers understandably and rightfully deplore.

Some companies have argued that software that does not meet a strict, narrow definition of spyware (system monitoring, data gathering, backdoor connectivity) should be excluded from the discussion of spyware. Were we to do so, we would ignore the vast majority of problems that consumers experience with unwanted commercial software. In fact, some the more widely distributed (and despised) forms of advertising software may not meet a strict definition of spyware, however, this software usually engages in other abusive behavior such as:

- installing on PCs without users' full knowledge, consent, and understanding;
- making unwelcome modifications to users' systems and web browsers to drive users to online commercial sites and services;
- adding unwanted toolbars and other widgets to users' browsers and systems;
- displaying unsolicited advertising on users' desktops through pop-ups that interfere with consumers' everyday use of their PCs;
- preventing users from reversing the changes made to their systems and browsers;

All of these problems warrant attention from the FTC, and we should not let distributors of unwanted commercial software define their products out of the discussion by insisting on a narrow, self-serving definition of spyware -- a term with a problematic usage history. If another term or name is needed for the kinds of software that consumers are complaining about, then let us find it.\* The problems that consumers face with unwanted advertising software are too serious to be dismissed on the basis of a mere definition dispute.

\* Note: for a discussion of one possible replacement for the term "spyware," see my "Junkware: A New Name for Spyware," included with these comments.

***2. Software that presents users with a EULA is adware, not spyware, and users elect to install such software on their systems.***

Spyware companies have resorted to another similar argument over the term "spyware" to insist that their software be excluded from the discussion of problems associated with spyware. On this argument, software that requires users to click through a EULA (end user license agreement) or similar legal agreement cannot be considered spyware because users' acceptance of the terms of a EULA allegedly indicates their awareness and understanding of the software. Such software is not "spyware," it is argued, but rather "adware," a seemingly innocuous form of commercial advertising software.

There are any number of problems with this argument, not the least of which is the unwarranted assumption that users who click through license agreements are fully aware (or could even become fully aware) of the software's true purpose and functionality. All too many of the EULAs that consumers encounter with unwanted software are presented in confusing, pressured circumstances -- in the midst of several pop-ups from a web site that refuses to work unless the user installs the correct plug-in, for example.

Moreover, these EULAs often couch complex, even outrageous, terms of agreement in long, dense blocks of legalese that few consumers have any hope of understanding. Many of these EULAs point to still more EULAs from other associated parties, requiring users to track down and plow through a pile of prose so daunting that few would ever venture to attempt it.

Still worse, some users may not even see the EULAs. Spyware companies often distribute their software through automated installations of ActiveX controls on web sites. These automated installations -- referred to by many users as "drive-by-downloads" -- are initiated by the web pages that users visit or the pop-ups spawned from those pages, not the users themselves. When web sites initiate program installations, users may or may not see a EULA. Whether they see a EULA is dependent not only on consumers' ability to use the meager amount of information provided Microsoft's Internet Explorer web browser, but also on the security settings for the Internet zone within Internet Explorer.

Internet Explorer provides users with information about ActiveX programs installed via "drive-by-downloads" and the software vendors responsible, however, this information is often not helpful in

determining the potential risks of ActiveX programs. With the default Internet zone settings users should see an Internet Explorer dialog box requesting their agreement to the installation of a program (i.e., an ActiveX control). Though this dialog box is titled "Security Warning," it provides almost no specific information that might help users understand the programs to be installed on their computers. Nor does it contain any strong warning that might alert users to potential privacy and security problems with this program. Although, this "Security Warning" box also provides a clickable link for users to get more information about the program -- usually the EULA -- it is quite easy for users to miss that information link. If users don't click the link, they won't see the EULA.

Some "drive-by-downloads" are initiated by web pages or pop-ups that do provide more information about the ActiveX controls, however, that information is usually not helpful in assessing privacy and security risks (it's usually promotional puff and hype). Moreover, if users are inundated with multiple pop-ups from a web page, they may not correctly associate the "Security Warning" box with the pop-up that caused it and may even think the program issues from the web site they are visiting, which may be a trusted source.

Given the poor quality of information presented to users during "drive-by-downloads" as well as the confusing manner and context in which that information is often delivered, it is not at all surprising that users would think nothing of clicking through Internet Explorer warning boxes without the slightest idea that they might be allowing intrusive spyware onto their systems.\*

If the security settings for the Internet zone are low enough, however, users won't even see the "Security Warning" box (let alone the EULA) -- the ActiveX controls or programs will simply install automatically. It is not uncommon for users to lower the security settings for Internet Explorer's Internet zone (the default security zone for all web sites) in order to get relief from the barrage of confirmation prompts (including the ActiveX "Security Warning" boxes) that result from surfing the web with the default Internet zone settings. Users simply do not understand that by lowering their Internet zone settings they are effectively rolling out the welcome mat for unwanted software, which can then install on their systems with no prompt or warning whatsoever.

It is difficult to imagine that spyware distributors are unaware of the problems that users experience with automated "drive-by-downloads" and complex EULAs that few people can make any sense of. When spyware distributors couple dense crops of legalese with disorienting "drive-by-downloads," the effect on confused consumers is not unlike the bewilderment created by the fast-talking door-to-door salesman who gets his foot in the door and, in a flash, is in your living room, busily vacuuming the carpet and arranging shelf space for a new set of encyclopedias.

These companies benefit enormously from such confusion, as many of them have business models that are built upon the widespread distribution of their software -- even to consumers who might not normally be interested in their programs. Spyware distributors have no business exploiting users' ignorance of computers and the law -- a deadly combination, to be sure -- only to claim that consumers' complaints ought to be ignored because users somehow "elected" to install their companies' software.

The sad fact is that we would not even be discussing the problems with spyware if spyware distributors started providing better notice to users and stopped distributing their software through means and methods that they surely know are likely to cause complaints from consumers.

\* Note: for a more detailed discussion of the problems with "drive-by-downloads," see my "The Anatomy of a Drive-by-Download," included with these comments.

## Distribution of Spyware

### ***3. If users would stop surfing porn sites and crackz/warez sites, the spyware problem would solve itself.***

When consumers visit web sites associated with pornography (porn sites) or pirated software (warez/crackz sites) they are certainly more prone to encounter unwanted, abusive spyware. Plenty of users, however, pick up spyware by visiting completely "legitimate," "mainstream" web sites or by installing apparently innocuous software from seemingly reputable sources.

If porn sites and warez/crackz sites were to disappear from the web tomorrow, we would still have a spyware problem. Indeed, spyware distributors would likely ramp up their efforts to distribute their software through more "mainstream" web sites frequented by large numbers of consumers.

Finally, it is well known that the online porn industry serves as a kind of "test bed" for new technologies and business practices. Technologies and practices that were once the exclusive province of porn sites just a few years ago are now commonplace on the "mainstream" internet. Moreover, as any number of spyware distributors themselves have argued, spyware could very well become an attractive means for large, "mainstream" online entities to push their commercial messages on users, especially given the problems that have plagued the online advertising industry over the past few years.

### ***4. If users would stop installing P2P file-sharing applications, the spyware problem would solve itself.***

As with porn sites and warez/crackz sites, consumers who carelessly download and install popular P2P (peer-to-peer) file sharing applications could find that they have also installed spyware that was bundled with those host applications. The potential risk of P2P file sharing applications is a red herring, though -- at least for the purposes of our discussion of spyware. There are plenty of P2P file sharing applications that do not bundle spyware. Moreover, consumers face the threat of spyware from many other sources. P2P file sharing applications could be driven from the Net tomorrow, and consumers would still face a problem with spyware.

### ***5. Users can easily prevent spyware from being installed, so it's their fault when it is installed.***

There are indeed several anti-spyware software packages that allow users to prevent the installation of spyware on their systems. Some of the better ones include JavaCool's SpywareBlaster and SpywareGuard, the SpywareGuide ActiveX block list, the several custom-built HOSTS files available on the Net, and my own utilities for Internet Explorer (IE-SPYAD and Enough is Enough!). Moreover, users can customize their Internet Explorer security zone settings to "lock down" Internet Explorer and guard against the installation of unwanted spyware. These preventative approaches, however, all have problems that could make them unsuitable for many, if not most internet users.

First, many of these preventative approaches are too complex for average internet users to employ. These prevention methods often demand a familiarity with computers and a set of skills that are simply beyond what most users could be expected to acquire. Still further, they require users to master a complex set of trade-offs between privacy and security (on the one side) and convenience and usability (on the other), and the technical act of balancing of these trade-offs can challenge even the savviest of computer users. Even the simpler preventative solutions confront users with a potentially steep learning curve.

Second, most of these preventative approaches leave consumers vulnerable to new forms and versions of spyware, much as anti-virus programs leave users vulnerable to new viruses, worms, and trojans (at least until updated signature definitions are installed). Spyware distributors have become increasingly aggressive in pushing their unwanted software on users, frequently (sometimes even daily) modifying and morphing their software to bypass anti-spyware applications. Still worse, spyware distributors have been developing ever more complex and sophisticated means to foist their software on users' systems, much as spammers have resorted to ever more byzantine methods to get their unwanted bulk commercial email past spam filters. In some cases, these newer distribution methods have proved so complex that it takes dedicated anti-spyware developers days, and even weeks, to develop a response.

In such an environment, average internet users have not a chance of protecting their systems. And note that we haven't even begun to discuss spyware distributors who use deceptive or even fraudulent pop-ups (e.g., fake error boxes and system notices; prompts to install false "updates" from Microsoft, et al) as well as confusing graphical interface elements (e.g., mislabeled or misleading buttons and hyperlinks, uncloseable popups, et al) to trick users into installing software. Still other spyware vendors exploit known security holes in Microsoft's software to automatically install their programs on consumers' PCs.

Finally, in a troubling turn of events, spyware distributors are increasingly and noisily complaining that anti-spyware developers interfere with the installation of their software. It is not unreasonable to expect that spyware distributors might very well resort to the court of law to ensure that consumers have no recourse whatsoever to third-party spyware-prevention methods and tools.

## **Effects of Spyware**

### ***6. Spyware isn't a significant problem because users can install anti-spyware applications to protect their PCs.***

The anti-spyware market has grown by leaps and bounds over the past few years, and consumers certainly have a number of spyware removal applications to choose from. Among the several excellent free spyware removal tools are Lavasoft's Ad-aware Personal and PepiMk's SpyBot Search & Destroy. There are also several for-pay applications such as PestPatrol and Webroot's Spy Sweeper. Big-name anti-virus vendors like McAfee and Symantec have also entered the market recently. Despite this wealth of anti-spyware scanners (which work much like more traditional anti-virus scanners), many consumers will not find these programs to be a satisfactory solution to the problem of spyware.

First, as was the case with spyware prevention methods, these scanning programs are much too complex for many consumers to use properly and effectively. The root of this difficulty stems from the complex nature of the spyware problems that these anti-spyware applications flag for users. So daunting are the scan results from anti-spyware applications, that it is not uncommon to find users who have installed and run an anti-spyware application on their computers only to balk at fixing problems because they are too intimidated to do so.

Second, because of the complex and fast-changing nature of spyware, consumers will often have to resort to several anti-spyware applications to clean their systems properly. Despite the excellent quality of the better known applications, no single one of them will do the job by itself. Thus, consumers must learn to use not one but several new applications. Some of these spyware removal applications may be highly specialized, such as Merijn's CoolWebShredder or Javacool's RapidBlaster Killer. These specialized tools are designed to remove particular types of spyware and are frequently updated to keep pace with the applications they target.



What's worse, even a combination of standard anti-spyware scanners may not be able to fix all of the spyware problems on consumers' PCs, especially when dealing with very new and sophisticated types of spyware. In such cases, users may have to download HijackThis! (a free program that logs key system settings) and post a HijackThis! log to an online forum for experts to review. All too many users will simply be unable to go through such a long and difficult journey to remove unwanted spyware from their systems.

Third, some spyware applications now block the download of anti-spyware utilities and deny users access to anti-spyware resources on the Net where they could get help. There have also been a small number of spyware applications that have maliciously uninstalled anti-spyware tools on users' hard drives or sabotaged them to prevent their use. Average consumers unfortunate enough to be victimized by one of these vicious spyware applications are utterly at the mercy of spyware vendors because they are denied the tools and resources to establish control over their own computer systems.

Fourth, anti-spyware scanners have many of the same shortcomings as spyware-prevention methods. The protection they offer always lags, to some extent, behind the newer spyware threats that appear on the Net almost daily. Given that some spyware applications are known to break users' internet connections or even block access to anti-spyware resources on the Net, consumers can easily fall prey to new forms of spyware that their anti-spyware scanners do not recognize, only to be denied access to the updates or online assistance that would allow them to remove that unwanted spyware.

Fifth, anti-spyware scanners only fix problems after the toll has been exacted on users' PCs and the damage done. No anti-spyware scanner can give back to users the lost, frustrating hours during which they were denied the use of their computers and forced to clean up after intrusive, unwanted software.

Sixth, we should also note that the uninstallers provided by spyware vendors themselves are not a viable solution either -- at least not in their current forms. As discussed earlier, not only do many spyware applications lack uninstallers, but the vendor-supplied uninstallers that do exist often fail to remove the associated applications completely. Consumers must have access to those uninstallers if they are to use them, however. Many uninstallers are offered only on vendors' web sites and are not included with the installed applications. As consumers often will not be able to identify the source of unwanted software on their systems, they won't be able to locate and access the vendors' web sites to download the uninstallers (which are frequently tucked away in obscure corners of those sites). And as was the case with the student I helped recently, uninstallers available on vendors' web sites do no good at all when spyware breaks the user's internet connection. Given the hoops that some spyware vendors force users to jump through in order to uninstall their applications, it is difficult to come to any other conclusion but that these vendors go out of their way to deliberately discourage and even prevent users from removing their unwanted applications.

Finally, as we noted earlier when discussing spyware-prevention methods, spyware distributors are becoming more aggressive in going after anti-spyware vendors, complaining loudly about the interference with their software, and even threatening legal action against anti-spyware vendors. Given such a hostile environment, it is an open question whether anti-spyware vendors will continue to be able to provide users with effective spyware detection, protection, and removal.

Anti-spyware vendors offer critical resources for consumers who are cleaning up their systems after a bout with spyware. As welcome as these resources are, they are no substitute for strong consumer protection against the more abusive and dangerous practices of the spyware industry.

***7. Spyware is just another form of advertising that helps support free content on the Net; anti-spyware applications that block or remove spyware undermine the implicit contract between internet surfers and the web sites they choose to visit for free.***

What is surprising and frustrating about this argument is that it flies in the face of so many of the other excuses offered for spyware distributors and commercial advertisers more generally. The commercial advertising industry has long argued that consumers need no federal legislation to protect their privacy on the Net because consumers have access to software applications to protect themselves. Private market solutions, we have been told over and over, are far preferable to intrusive governmental mandates. On this earlier argument, privacy and security software gives consumers choices and thus negates the need for governmental intervention in the marketplace.

As we noted above, the anti-spyware market has indeed exploded in response to consumer complaints about spyware (even if problems with anti-spyware tools remain). Confronted with a free market solution to the problem of spyware, however, the spyware industry now suggests, incredibly enough, that such private solutions are illegitimate and perhaps even illegal. Where the commercial advertising industry once headed off privacy legislation by pointing to the choices offered consumers in the free market of software tools, the spyware industry (a part of the larger commercial advertising industry) now appears to insist that consumers ought to be denied the use of such tools.

No solution to the problem of spyware, it would seem, is acceptable to the spyware industry. It argues that its software ought not be subjected to governmental regulation because that software does not meet a narrow, self-serving definition of spyware; it argues that consumers "elect" to install its software, only to insist that consumer complaints be ignored; it blames consumers for being ignorant and careless in maintaining their systems, only to insist that consumers have enough privacy protection by virtue of the many anti-spyware applications on the market. After all this, however, the spyware industry then hints that those very same free market solutions and choices might themselves be illegitimate.

What lies at the end of this sorry litany of excuses and protests is an arrogant, offensive, and even dangerous assumption: namely, that consumers are ethically (and perhaps even legally) obligated to submit themselves and their systems to intrusive advertising software; that consumers' computer systems ought to be open for hijacking and use by commercial advertisers; that internet users and citizens are obligated above all else to become passive eyeballs for whatever online advertisers choose to put in front of them; and that, finally, consumers and citizens ought to have no choice or say in the matter. Were we to accept such a proposition, we would effectively reject any hope that the internet, with all of its portent and promise, might become (or even remain) a vital communications medium for citizens. Instead, it would degenerate into merely another passive medium in which disempowered consumers -- not engaged and active citizens -- are subjected to the whims of dominant commercial interests. I would hope that the FTC would see clear to avoid this outcome by protecting internet users from the more unscrupulous demands and tactics of commercial advertisers.

***8. The spyware "controversy" has been concocted by greedy anti-spyware companies to cash in on users' fears and paranoia.***

This myth or excuse can be only be described as amusing. Presumably the spyware industry would have us believe that internet users would be perfectly happy with broken PCs, hijacked browsers, and pop-up infested desktops, if only the anti-spyware industry would just be quiet about it. We would also have to believe that the millions of users who have downloaded anti-spyware applications and have flocked to anti-spyware sites for help and advice are simply deluded -- that the problems are all in their heads, and that anti-spyware vendors planted those nefarious delusions in what would surely count as one of the

more stunningly successful propaganda or public relations campaigns of the past hundred years. Such is the heady, noxious stuff of self-serving fantasy, and anyone who has actually worked with users whose PCs have been trashed by intrusive spyware will surely recognize that the spyware industry is simply blowing smoke.

But not completely. In a strange twist of circumstances, the spyware industry does have a point -- but not quite the point it thought it had. There are indeed unscrupulous anti-spyware vendors on the Net who resort to high pressure sales tactics and who prey on users' fears and cash in on their paranoia by springing cheap scares (e.g., opening users' CD-ROM trays, "exposing" the contents of their C-drives, et al) on gullible web surfers. Not surprisingly, many of the anti-spyware applications from such vendors turn out to be so much snake-oil. Prone to "false positives" and yet seriously deficient in detecting real spyware threats, these "rent-a-coder" anti-spyware applications flag non-existent problems on users' computers and then demand payment to fix them -- a classic con game.

These rogue anti-spyware applications, however, do not emanate from the well-known anti-spyware vendors, advocates, and activists who have earned users' trust over the past four years. Rather, they often issue from elements of the advertising and marketing industry itself including, incredibly enough, companies that are known to distribute spyware. These rogue applications even fool users by trading on the trusted names of legitimate anti-spyware programs (e.g., "spybot") in their advertising through Google's "Ad Words."

Thus, it is true in some sense that the spyware problem was concocted by anti-spyware vendors. Not only have some rogue anti-spyware vendors distributed the very types of software they promise to clean off users' computers, but unscrupulous elements of the advertising industry have rushed in to the market to exploit users' fears. Legitimate, trusted anti-spyware vendors such as those I mentioned earlier, however, have played no part in this charade. In some cases, they have even been the victims.

## **Solutions to Spyware**

### ***9. Once users are educated about spyware, the spyware problem will solve itself.***

If there has been one common theme throughout this discussion of "spyware myths," it has been that normal, average, everyday, non-tech-savvy internet users are at the mercy of aggressive spyware distributors who do everything in their power to foist unwanted software on these vulnerable consumers.

Rather than rehash the many relevant points once again, let me point to an interesting, and ultimately depressing, experiment in computer user education that has been going on for some ten years. I am, of course, referring to the problems of traditional malware -- viruses, trojans, and worms -- as well as the inability of normal computer users to learn safe computer behavior or even to use anti-virus applications properly and effectively to defend their PCs. Anti-virus applications have been around since the late 1980's, and viruses and worms slightly longer than that. Of all the privacy and security problems that face consumers, traditional malware is the most familiar to them. Moreover, of all the myriad privacy and security applications on the market, anti-virus programs have achieved the highest levels of market penetration and consumer adoption.

One would think that after ten plus years of ongoing efforts to educate computer users about the threat of malware and the proper use of anti-virus applications we could expect results -- perhaps only modest evidence of small steps towards improved security, but tangible results nonetheless. As the unprecedented wave of viruses and worms over the past year should have demonstrated, such is not the case. Some five years after the first mass email worm rocketed around the internet, many users are all too willing to open unknown attachments. And over ten years after anti-virus applications were introduced to the consumer

market, many computer users still do not understand that they must update their anti-virus application's virus definitions; nor do they even know how to perform a manual scan of their hard drives. (Anyone who works with average computer users should be able to confirm the truth of these grim assessments.)

I am an educator by profession and choice. If anyone regards education optimistically, it is I. Indeed I already spend a good deal of my time attempting to educate users about spyware problems. As noted just above, however, this ongoing experiment in computer user education is both highly suggestive and extremely depressing in what it tells us. We would be wise to heed the lessons here and resist the urge to place too much faith (or find too many excuses) in the prospect that users might solve the spyware problem themselves by simply getting educated about it.

***10. Once the industry develops a "self-regulation" plan, the spyware problem will solve itself.***

As noted earlier, the problem of spyware is but the most recent stage of a longer struggle over the best ways to protect consumers' privacy online. At earlier stages in this struggle, the internet advertising industry (along with other online commercial interests) rejected federal regulation and insisted that a "self-regulatory" market solution would be far preferable and even more effective as a means for protecting consumer privacy. After successfully fending off most privacy legislation, the advertising industry turned to the task of crafting a plan for "self-regulation." What the industry came up with, however, has been something less than a smashing success. Faced with serious consumer complaints about privacy violations, the industry essentially declared, "Let them eat privacy policies!" Even the addition of a meager supplementary diet of P3P compact policies and third-party trustmarks has done little to satisfy or assuage consumers' privacy concerns.

When we consider the threat of spyware, the problems with industry "self-regulation" remain the same. It is simply not realistic to expect that an industry would suddenly learn the virtues of self-restraint when that industry stands to benefit enormously from the widest and most intrusive distribution of its software possible. That this same industry is now making noises to the effect that consumers are obligated to accept its advertising software and that anti-spyware applications are illegitimate intrusions into the marketplace should be still further cause to doubt the ability of this industry to regulate itself.

## **Conclusion**

As this has been a long discussion, I will keep my concluding remarks brief. The FTC now confronts a problem that is quickly becoming the most significant threat to the ability of consumers and citizens to use their computers and the internet in a private and secure manner. It also faces an industry which is largely unrepentant about what it does and the way it does it -- an industry arrogant enough to suggest that consumer complaints are largely a figment of the imagination and that internet users have no choice but to accept its unwanted, intrusive offerings. I sincerely hope that the FTC would see through such bluster and excuse-making and find a way to offer citizens and consumers the protection they need.

Respectfully submitted,

Eric L. Howes

# "Junkware": A New Name for "Spyware"

by Eric L. Howes

The name "spyware" was first used to describe unwanted commercial software during the spring and summer of 2000, when consumers became aware of "adware" -- advertising sponsored "freeware" -- which often monitors system use and report potentially sensitive data to advertisers for the purpose of targeted advertising. The name "spyware" proved to be a catchy one, and consumers were soon using it to describe or name all manner of unwanted software that engaged in unwelcome behavior -- even software that did not technically "spy" on users. In other words, the term "spyware" has become a loose, broad term used by consumers for a wide variety of unwanted, intrusive software that they understandably and rightfully deplore.

Although the name "spyware" has proved popular with internet users, it has caused more than its share of confusion because the term implies functionality (data gathering, backdoor connectivity, etc.) that some intrusive, unwanted software may not have. Not only have vendors of certain kinds of "advertising software" vociferously protested the application of the name "spyware" to their software, the name "spyware" has also caused users to confuse commercial advertising "spyware" with more traditional "spyware" such as keyloggers and other system monitors -- electronic snooping tools that differ markedly from commercial advertising "spyware" in that these snooping tools are deployed and used by individuals acting in their own interests, not by the companies who develop and distribute those tools.

Given that the name "spyware" has been overextended and is now only causing pointless confusion and useless haggling that distracts us from the crucial business of addressing the very real problems that consumers face with certain types of software on the internet, it is time that the name "spyware" be replaced with another one that more readily encompasses all the varieties of unwanted, intrusive commercial software that consumers are complaining about (and which they problematically lump together under the term "spyware").

While it will be difficult to find a replacement quite as catchy as the name "spyware," one possible replacement is "junkware."

## Varieties of "Junkware"

By "junkware" we mean unwanted, commercial software that is installed without the user's full knowledge, consent, and understanding, and that primarily serves the interests of commercial parties associated with the "junkware," not the end users on whose systems those unwanted applications are installed. The term "junkware" covers such applications as:

- **adware:** "advertising supported software" -- i.e., "free" software that is supported by the display of advertising -- often within the main window of the application -- or the use of the user's PC for other commercial purposes (e.g., distributed computing). This advertising is often accompanied by the collection and transmission of marketing and demographic data for the purpose of targeted advertising, which makes such applications spyware as well (see below for a definition of spyware). Although the software is billed as "free," the user in fact

"pays" for the application by putting up with advertising as well as the collection of data (often about the user's behavior with the application or on the internet). Moreover, although the user typically clicks through EULA, thus consenting to this advertising and data collection, many (if not most) users are unaware of the true functionality of this software.

- **foistware**: commercial software that piggybacks on "free" software (a "host") and is installed along with the host application (such as KaZaA or Grokster). An alternative to straight "adware" that serves the same function, "foistware" often displays ads or collects marketing and demographic data for use by direct marketing companies, in which case such applications are spyware as well (see below for a definition of spyware). These piggybacking applications are referred to as "foistware" because they are unwanted by the user. Although users may have technically (legally) agreed to the installation of these "foistware" components during setup of the host application by clicking through a EULA, many (if not most) users are either unaware of these foistware applications or do not fully understand them.
- **spyware**: commercial software that monitors users' computer and Internet behavior, gathers other marketing and demographic data, and transmits those data to direct marketing and advertising firms, who often use those data for targeted advertising. Collected data may include personally identifiable or sensitive information, as well as information about users' internet behavior, computer usage, and usage of the application. Note that by the term "spyware" we do not mean such applications as keystroke loggers (keyloggers) or other similar system monitors that are used to snoop on users. Those applications do not have a marketing or advertising tie-in or use; commercial/marketing "spyware" does. (Note also that the term "spyware" here represents a subset of the larger category of unwanted software that I propose be called "junkware"; it is not used as a general term for all manner of unwanted, intrusive commercial software, such as the term is currently used among internet users and consumers.)
- **hijackware**: applications or web sites that set the user's default browser home page to an unwanted URL, change the default search engines defined within the browser to unwanted search engines and sites, or add unwanted toolbars and other custom plugins/add-ons to the user's browser and system. These applications and web sites may also configure Windows to prevent users from changing those settings back to the users' preferences or uninstalling the unwanted toolbars and plug-ins/add-ons. These applications and web sites may also edit the HOSTS file to tie known web sites to certain IP addresses, thus ensuring that users are unwittingly directed to unexpected, unwanted web pages.
- **drive-by-downloaders**: unwanted applications that install automatically when the user visits a web site. These are usually ActiveX controls and plug-ins, and users may or may not (depending on their Internet Explorer Security zone settings) see a pop-up requesting agreement to a EULA that authorizes installation of the application. In all cases, though, the download is initiated by the web site being visited, not the user.
- **porn dialers**: applications that employ users' modems to dial 1-900 numbers (often overseas) and connect with online services that distribute porn. The 1-900 phone charges that result

from these phone calls are usually astronomical and outrageous. Moreover, these porn dialers are often installed via "drive-by-downloads," and users are frequently unaware that their modems are even being used to connect to 1-900 numbers (they find out later when the phone bill arrives).

There are many other terms that people have coined for these types of "junkware," however, "junkware" is a comprehensive term for all of these types of unwanted, intrusive commercial software.

Keep in mind that any one application may fulfill several of the above definitions. Thus, there can be "adware" that is also "spyware." There may be "drive-by-downloaders" that are both "spyware" and "hijackware." And so forth.

"Junkware" is often distinguished from other (more traditional) forms of malicious software such as viruses, trojans, and worms by the fact that, in most cases, the user clicks through a EULA (end user license agreement) at some point -- by contrast, no virus will ever ask you to agree to a EULA. Thus, the companies who push "junkware" on users can claim that users "elected" to install their applications. Nonetheless, this "junkware" is unwanted by and unknown to users even though they may have technically (legally) agreed to the installation of that software.

## **What "Junkware" Does**

"Junkware" is a broad term that covers a wide variety of unwanted software applications that are pushed on users. "Junkware" often does one or more of the things:

### ***Stealth/Rogue Installation***

- automatically installs with little notice or warning when users visit "junkware"-infested web sites with active content options enabled, as many sites require them to be;
- tricks users into installation by the use of deceptive buttons and hyperlinks, false error boxes and system notices, uncloseable popups, or other confusing GUI elements;
- falsely poses as Microsoft Windows Update software, "anti-spyware" software, or other software that may be desired by users;
- uses known "malware" such as the W32.Dlder.Trojan and/or exploits known security holes in Internet Explorer and Windows to install on users' systems and reconfigure users' systems;
- piggybacks on other host applications and web sites which install the accompanying "junkware" modules -- even when users uncheck the appropriate boxes and decline the installations -- and often provides no visible means to opt-out of the "junkware" installation alone;
- uses frequently changed/morphed installers and installation methods to avoid detection by "anti-junkware" applications such as SpyBot Search & Destroy and Ad-aware;

### ***High Pressure Installation***

- foists itself on users by piggybacking on other host applications which require installation of that "foistware";
- uses scare tactics (e.g., displays of users' drive contents, IP addresses, or browser headers; opening the CD-ROM drive) to exploit users' fears and pressure them into installation;
- is required by ISP's in order to provide "member content" and "connection maintenance" to users;
- installs along with drivers for hardware and is required for proper functioning of that hardware, or installs as part of a BIOS/CMOS software package;

### ***Stealth Execution***

- configures itself to automatically launch and run silently in the background every time Windows or Internet Explorer start without notifying users or seeking their knowing consent;
- obscures or hides its execution and behavior from users and "anti-junkware" utilities;

### ***Rogue System Reconfiguration***

- reconfigures users' systems to allow itself unfettered access to the Internet and allow "junkware" servers uninhibited access to users' computers;
- hijacks users' web browsers to drive users to unwanted web sites and search services by making undesired system customizations and locking users out of the settings that would allow them to restore their browsers to a preferred state;
- adds unwanted or unsolicited toolbars, searchbars, and other custom plug-ins or add-ons to the users' browsers or systems;
- replaces critical Windows system files, thus interfering with the normal and proper operation of the users' systems and even imposing a system "death penalty" on the PCs of users who do attempt to uninstall it;

### ***Data Gathering***

- monitors users' use of their computers and the internet, collects usage data and other personally identifiable or sensitive data about users, and provides those data via a network connection to direct marketing and advertising companies;



### ***Backdoor Connectivity***

- establishes unannounced, unwanted network connections for the purposes of making unrequested updates to the software and users' systems or supplying data to interested parties;
- makes unauthorized dial-up connections to 1-900 numbers without users' full understanding and consent;

### ***Obfuscation***

- buries key notices, terms, and conditions in complex EULAs and Privacy Policies that few consumers can make any sense of;
- provides insufficient notice of installation, data gathering, backdoor connectivity, system reconfiguration, or other undesirable behavior;

### ***No Choice (Opt-Out/In)***

- won't take "no" for an answer because it provides no readily available means to opt-out of (let alone opt-in to) privacy invasive data gathering, system reconfiguration, and/or system updating for good;
- demands that consumers to agree to outrageous terms & conditions such as the acceptance of unannounced / unsolicited updates, renunciation of third-party uninstallation methods (i.e., the use anti-"junkware" utilities such as SpyBot Search & Destroy and Ad-aware), or the uninstallation of "conflicting" programs (i.e., anti-"junkware" utilities such as SpyBot Search & Destroy and Ad-aware).

### ***Uninstallation Countermeasures***

- provides no visible means for uninstallation and removal;
- refuses to be uninstalled when the host application is uninstalled;
- provides broken uninstallers or uninstallers that actually install more "junkware";
- takes active measures to avoid being uninstalled by "junkware" removal utilities like Ad-aware and SpyBot Search & Destroy, blocks the download and installation of those utilities, and even silently uninstalls such utilities without the user's permission;

### **Other Definitions of "Spyware" or "Junkware"**

Others in the "anti-spyware" scene or industry may classify software applications differently than I do. See in particular the following web pages...

**SpyBot Search & Destroy - Target Policy (Patrick Kolla)**

<http://security.kolla.de/index.php?lang=en&page=knowledgebase/targetpolicy>

**SpywareGuide.com**

[http://www.spywareguide.com/category\\_list\\_full.php](http://www.spywareguide.com/category_list_full.php)

**Lavasoft Threat Assessment Chart**

<http://www.lavasoftusa.com/support/resources/>

**and.doxdesk.com - Parasites**

<http://www.doxdesk.com/parasite/>

**Kephyr - Spyware**

<http://www.kephyr.com/spywarescanner/library/glossary/spyware.phtml>

**Webopedia.com - Spyware**

<http://www.webopedia.com/TERM/s/spyware.html>

...for other attempts to classify and define all the varieties of "junkware" (a.k.a, "spyware"). Note that some of the software described on those pages may be more traditional "malware" (i.e., viruses, trojans, worms).

## Conclusion

Some may object to the name "junkware" because of the unpleasant connotations that it carries. If another more satisfactory name can be found, then it should be adopted. The important thing, however, is that we not let a dispute over a misused word like "spyware" distract us from the very important business of addressing the problems that consumers are complaining about when they encounter a broad class of unwanted commercial software on the internet, whether we call that class of software "spyware," "junkware," "greyware," "ad-ware," "bad-ware," "advertising software," "unwanted-ware," "mysteryware," or even "x-ware."

Definitions and terms ought to help us understand the world and grapple with the problems that it presents, not stand in the way of our efforts to solve those problems. When we are dealing with consumer complaints about intrusive, unwanted software on the internet, the particular name for that broad class of software is less important than the varieties of software that it allows us pull together under the umbrella of one term and discuss productively. Put another way, the particular name for that linguistic umbrella is less important than its ability to facilitate our attempts to address consumers' problems and concerns with the abusive software that falls under its cover.

29 March 2004

# The Anatomy of a "Drive-by-Download"

by Eric L. Howes

## Introduction

Spyware vendors frequently use automated installations of ActiveX controls (a special kind of plug-in program for Microsoft's Internet Explorer web browser) to distribute their software via web sites. These automated installations are initiated when web surfers land on pages that include HTML code to start the download and installation process. These installations may also be initiated by pop-ups spawned by web pages that users visit. As these installations are initiated by web sites and not users, many consumers refer to these automated installations as "drive-by-downloads." Web users often find these "drive-by-downloads" confusing and disorienting, and it is little wonder that many of them would carelessly click through pop-ups on web sites with very little understanding of the programs they are in fact allowing to be installed on their PCs. To appreciate fully why the spyware problem has gotten as bad as it has, we must understand the "drive-by-download" process and recognize just why it proves bewildering and misleading to consumers and how it coerces consumers to install software that they do not understand and might not want if they did.

In this document I walk through the process of a "drive-by-download," explaining how it works, what users see in the process, and why consumers might feel confused or misled by it. I also detail the effects of the software installed via this automated installation process on a test PC. Towards the end, I summarize the efforts required to remove that software completely from that PC.

Readers should keep in mind that the case I present here is but one example "drive-by-download" and might not be completely representative of other automated installation processes and software found on other web sites. Where possible I do highlight significant differences from other "drive-by-downloads" that I have seen and explain what other software and web sites do in similar situations. For the purposes of this example, however, I did choose to visit the web site of one of the more prolific and well known distributors of advertising software on the Net, and it is likely that many consumers would recognize the software and installation process that I describe. Thus, the "drive-by-download" process that I use here is somewhat representative of what users experience with automated installations of unwanted advertising software, often referred to by consumers as "spyware."

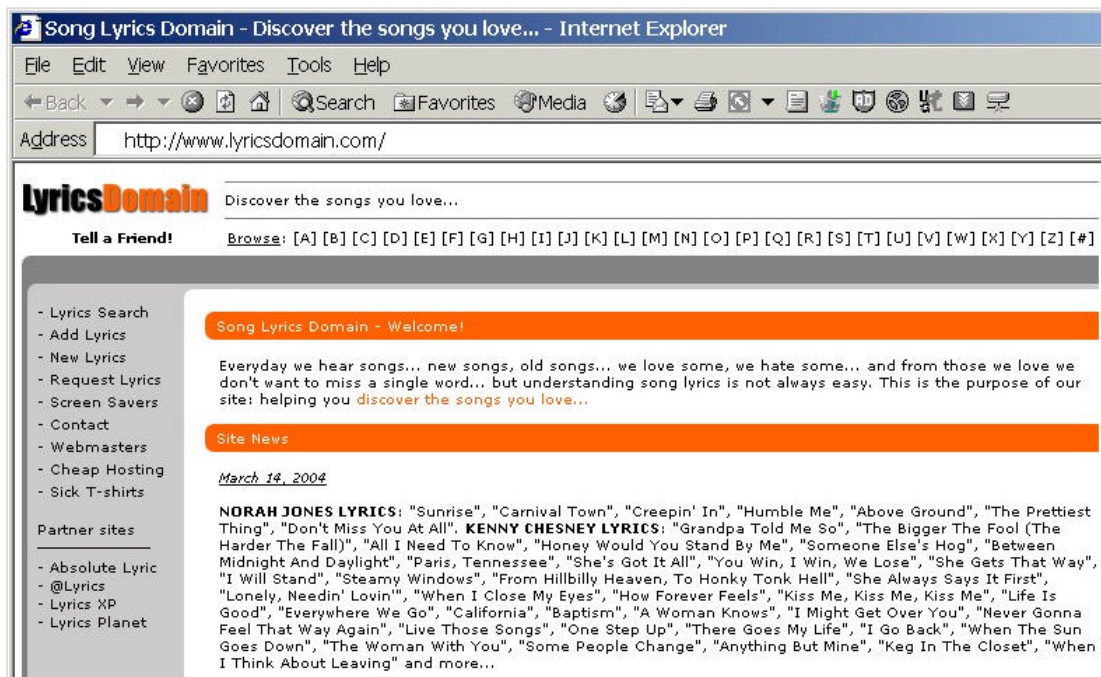
For this example "drive-by-download" I used an old, custom-built Pentium 166 PC with 64 mb RAM. It was loaded with Windows 98 SE and Internet Explorer 5.5 w/ SP2. Although this system is fairly dated in comparison with the systems now being sold by major OEMs, it is still quite usable. I deliberately kept the number of installed applications on this system to a minimum (thus, no Microsoft Office, for example). I also made minor configuration tweaks to the system to improve its responsiveness and performance. Internet Explorer's security zone settings were left at their defaults. Moreover, no privacy or security software (such as an anti-virus program, anti-spyware tool, or personal firewall) was running to protect the system. In sum, this was an older system, but one that would be similar to many that consumers are still running.

## The Installation

On March 23, 24, and 26, I visited a web site named LyricsDomain (<http://www.lyricsdomain.com/>). This web site purports to help users with the lyrics to popular songs:

Everyday we hear songs... new songs, old songs... we love some, we hate some... and from those we love we don't want to miss a single word... but understanding song lyrics is not always easy. This is the purpose of our site: helping you discover the songs you love... ([www.lyricsdomain.com](http://www.lyricsdomain.com))

In fact, it is a web site that distributes advertising software from C2 Media, known to many web surfers as Lop.com after one of the company's main web sites ("lop" stands for "live online portal"). There is nothing on the home page of the LyricsDomain site, however, that overtly indicates its association with C2 Media.



*Figure 1: LyricsDomain home page*

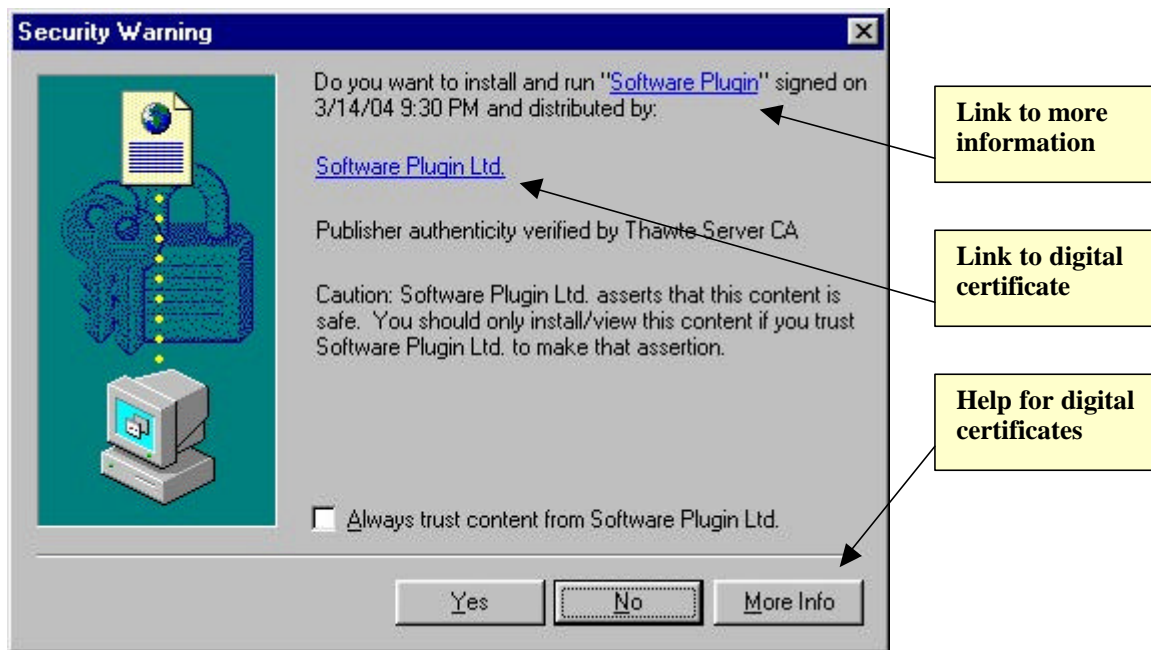
The site's privacy policy (<http://www.lyricsdomain.com/privacy.html>) is fairly innocuous and even appears to be "consumer friendly":

Privacy is becoming a major concern on the Internet now, because of the popularity of the Internet some businesses have taken advantage of the huge amounts of data they have collected through their web sites by 'spamming' or by adding you to annoying mailing lists which you don't even remember signing up to.

Lyrics Domain does not require you to disclose personal information anywhere on the site, so it's not a major problem. However in the event that we do adopt features to the site which require you to fill out forms requiring your personal information we will make it optional and we will never, ever make the information accessible to the public, sell it to anyone or use it for any purposes except for our own research. ([www.lyricsdomain.com/privacy.html](http://www.lyricsdomain.com/privacy.html))

Although I am familiar with lyricsdomain.com and the software that I would encounter there, many consumers will not be, and that lack of familiarity with the web site or C2 Media could very well play a crucial role in determining how average consumers handle the "drive-by-download" process at LyricsDomain.

When I landed on the LyricsDomain home page, I was almost immediately confronted with a "Security Warning" box from Internet Explorer:



*Figure 2: "Security Warning" for "Software Plugin"*

This is the standard warning box that Internet Explorer provides users for ActiveX controls loaded by web sites. Unless they have changed the security settings for the Internet zone in Internet Explorer, users should see this warning box whenever they encounter a page that attempts to install an ActiveX control on their systems. This particular warning box resulted from a hidden IFRAME (a window within a window) in the HTML of the LyricsDomain home page. That IFRAME loaded another small page (count.htm) that itself used JavaScript to begin the installation of a 12 kb ActiveX control named download.mp3.exe from lyricsdomain.com. As we shall see, this small ActiveX control was a stub downloader that would be used to download and install several megabytes of other software -- in total, eight different programs from at least three different vendors. That whole installation process, though, started with the automated installation of this small, innocuously named file described simply as "Software Plugin."

Despite its title, this "Security Warning" box contains very little information that would help consumers assess the potential privacy and security risks of the software to be installed on their systems or even to understand its purpose and functionality. The text chosen by the vendor to describe its software ("Software Plugin") is so generic and vague that consumers could easily mistake the software for a simple browser plug-in necessary to use the music content of the site.

In fact, this software has almost nothing to do with the content or functionality of this music site, but the "Security Warning" does nothing to indicate that. Moreover, it contains no strong language to warn users of potential privacy and security risks.

This warning box does contain two links (see Figure 2 above) which users can click to get more information about the program and to view the digital certificate of the vendor (misleadingly named "Software Plugin Ltd.") that digitally signed the software for distribution. Users might not recognize that those links are in fact clickable links, though. Even if they do, the information that they will get from those links is almost worthless. The information link for the vendor opens a new browser window to a page titled "Search the Web!" (<http://www.lop.com/>):



*Figure 3: "Search the Web!" home page*

Not only does this home page have no clearly discernible connection with the named software vendor ("Software Plugin Ltd."), but it contains no information at all about the software being installed. There is no EULA (end user license agreement) or any other information that might help the user understand the company or the nature of its software. Even at this stage there is no indication that C2 Media is involved in this process at all (though savvy internet users might recognize the domain name [lop.com](http://www.lop.com/)). There is a small "Help" link at the bottom of the page (not shown in Figure 3 above) that does take users to a page with information about C2 Media's or Lop.com's software (<http://www.lop.com/help.html>). It is doubtful that most users would even know enough to click that "Help" link, and those did could be forgiven for not understanding the relationship of the software described on that page with the "Software Plugin" being installed by LyricsDomain.

The "Security Warning" box does provide other means for users to get more information, almost none of it helpful. The link to the vendor's digital certificate brings up that certificate (see Figure 4 below), but it contains no useful information about the program itself. The "More Info" button

(see Figure 2 above) provides only a help page with generic information about digital certificates used to sign ActiveX controls -- again of little use to users attempting to make a decision about this particular "Software Plugin" and what it might do to their systems:



Figure 4: Certificate for "Software Plugin Ltd."

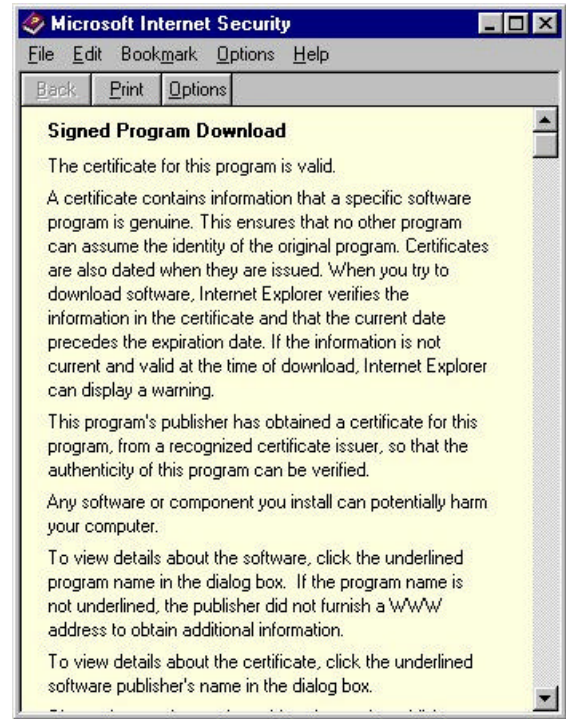


Figure 5: "More Info"

At this point we have seen nothing to indicate anything untoward or suspicious about the "Software Plugin." In fact we have gotten very little information at all. That situation changed dramatically once I clicked the "Yes" button in the "Security Warning" box (see Figure 2 above) and agreed to proceed with the installation. Another dialog box popped up with a license agreement (see Figure 6 to the right).

This license agreement is no simple matter. In fact, this license agreement for "Free Software Plugin" contains not one license agreement, but EULAs and privacy policies for three different companies. By clicking the "Accept" button in this "Verification Box," users are in fact consenting to the installation of a whole raft of software, not just the "Free Software Plugin."

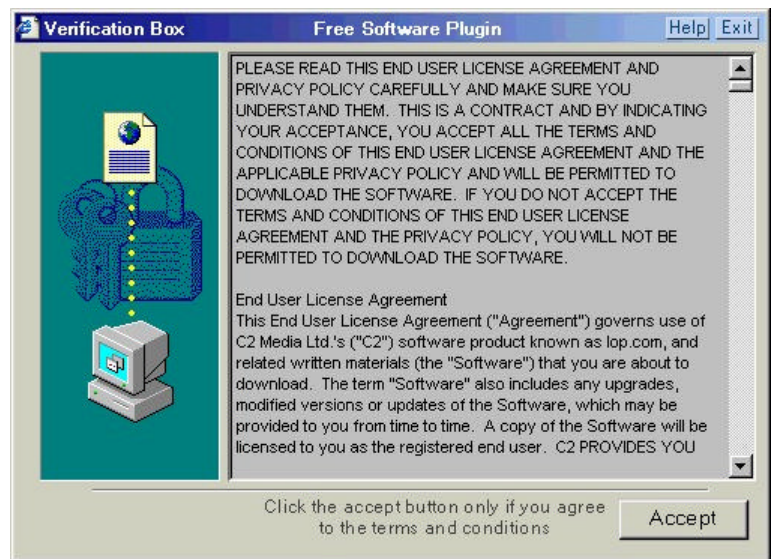


Figure 6: "Verification Box - Free Software Plugin"

Taken together, these various EULAs and privacy policies total almost eighteen single-spaced pages (thirty-six double-spaced). In 8400 words of dense legalese packed into numbingly long paragraphs, this agglomeration of licenses and privacy policies lays out a grim picture of the software to be installed on the user's system. What follows is a summary of the key terms (so far as I could make them out) contained in these documents:

<b>Company &amp; documents</b>	<b>Key software &amp; behavior...</b>
<b>C2 Media</b> <ul style="list-style-type: none"> <li>▪ license agreement</li> <li>▪ privacy policy</li> </ul>	<ul style="list-style-type: none"> <li>▪ Accessory Toolbar, Desktop Toolbar, Pass-Through Toolbar</li> <li>▪ browser configuration changes</li> <li>▪ advertisements; extensive system monitoring, data gathering/reporting</li> <li>▪ automatic updates</li> </ul>
<b>AdIntelligence LLC</b> <ul style="list-style-type: none"> <li>▪ license agreement</li> <li>▪ privacy policy</li> </ul>	<ul style="list-style-type: none"> <li>▪ "AdIntelligence AdServer" software (pop-ups/ pop-unders)</li> <li>▪ system monitoring, data gathering/reporting</li> <li>▪ automatic updates</li> </ul>
<b>Alset Inc.</b> <ul style="list-style-type: none"> <li>▪ license agreement</li> </ul>	<ul style="list-style-type: none"> <li>▪ HelpExpress (dialog ads)</li> <li>▪ Coupons and Offers (pop-ups)</li> </ul>

*Table 1: Summary of License Agreements and Privacy Policies*

It took me almost an hour to plow through these licenses and privacy policies in a careful manner and extract the key terms of the agreements, though even now I have to wonder if I caught everything significant and understood it properly. I think it entirely uncontroversial to state that this kind of document (or set of documents) could be read wholly and productively only by a practicing attorney -- and even then only one with endless amounts of time and patience.

We should also emphasize at this point that there was no reason in the world why these three vendors could not have supplied a more readable summary of the key terms of their software license agreements, such as I have done above. (We leave aside for now the issue of just why these companies would be distributing their software through an arrangement in which users consent to the installation of an innocuously named "Software Plugin" from a music lyrics site only to agree to the installation of several megabytes of other software, all completely unrelated to the functionality of a site named LyricsDomain.) I know of no average user who would have the faintest hope of getting through these documents, if indeed they ever tried.

What all too many consumers will do when confronted with such an impenetrable wall of legalese is do what I did: click "Accept" (see Figure 6 above).

Once I accepted the agreements, the stub downloader (download.mp3.exe) proceeded to download and execute a number of other installer programs. These executable installers ranged



in size from 228 kb to 1074 kb. As each one finished downloading, it proceeded to install various software programs on my system. New directories were created in C:\Program Files\ on my hard drive for these programs, though a few files were installed to C:\Windows and C:\Windows\System. New browser windows and pop-ups appeared as the freshly installed programs began running, and my system slowed dramatically, becoming increasingly sluggish as more programs executed and loaded into memory.

When the dust settled and the installation process finished, my PC was the unhappy new home to no less than eight different programs, not all of which were clearly flagged in the EULAs and license agreements that I had read. What follows is a summary of the programs installed on my system by the "Software Plugin" from C2 Media:

<b>Company</b>	<b>Program</b>	<b>Install Directory</b>	<b>In EULA?</b>
C2 Media	Window Active	C:\Program Files\Window Active	Yes
C2 Media	Window Searching	C:\Program Files\Pop User Jugs	Yes
C2 Media	ErrorOnce	C:\Program Files\Dead Remote	Yes
AdIntelligence	Apropos Media	C:\Program Files\SysAI	Yes
AdIntelligence	AutoUpdate	C:\Program Files\AutoUpdate	Yes
Alset	HelpExpress	C:\Program Files\Alset	Yes
Alset	Coupons and Offers	C:\Program Files\couponsandoffers	Yes
??	Rads01.Quadrogram	C:\Windows\	??

*Table 2: Installed Programs*

Some explanation of this breakdown of installed programs is in order. I have identified and classified the programs that were installed not only by examining the directories and files that were created on my hard drive, but by reviewing the license agreements and looking for key words. The uninstallation information contained in the Add/Remove Programs Control Panel applet proved useful as well, especially for determining the names of some applications. I have also based this classification on the scan results from SpyBot Search & Destroy and Ad-aware, two anti-spyware programs that I used to clean up my system (see the last section, "The Cleanup," for more details). In some cases I have consulted online resources in order to identify the programs for what they were. As a general rule I have regarded software as a clearly distinguishable program when it was installed in a unique directory (e.g., C:\Program Files\SysAI vs. C:\Program Files\AutoUpdate). Although each of those directories might have contained several executable files, I have still classified those files as a single program or application.

There is some doubt as to the identity of at least one of the programs installed. The Rads01.Quadrogram program was installed to the C:\Windows directory -- the only program file of its kind. It consisted of a single executable file (emsw.exe) that Ad-aware flagged as emanating from a unique "family" or vendor named Rads01.Quadrogram. Online research seems to cast doubt on that identification, though. Rads01.Quadrogram.com is a domain associated with the "Peper" trojan -- see the information from Network Associates ([http://vil.nai.com/vil/content/v\\_100635.htm](http://vil.nai.com/vil/content/v_100635.htm)) and Kephyr.com (<http://www.kephyr.com/spywarescanner/library/peper Trojan/index.phtml>). The "Peper" trojan uses random 14 character file names, not the emsw.exe file name. That file

name is reported to be associated with Alset HelpExpress -- see the information pages on "emsw.exe" from SysInfo.org (<http://www.sysinfo.org/>) and "HelpExpress" from PestPatrol (<http://www.pestpatrol.com/PestInfo/h/helpexpress.asp>). As I was unable to determine which of the several installers was responsible for installing this program, I am not certain whether this program was covered in any of the license agreements or privacy policies (thus the "?"). Whether the vendors involved in this package of downloads consider that program to be covered, I do not know; it is unclear to me even which vendor was responsible for putting that program on my system.

This seems a good point to emphasize the great difficulty in sorting out just what was actually installed on my system. It has taken considerable effort to sort through all of the newly installed files and directories and identify the programs as well as the vendors responsible for them. And despite its great length (8400 words), the collection of license agreements and privacy policies was of only minimal help in determining what had been installed and where.

The Apropos Media program is a good illustration of this confusion. That program was installed to C:\Program Files\SysAI, yet the installation program responsible for creating that directory was named AproposClientInstaller.exe. As there was no Add/Remove Programs entry to clarify the name of the program (as was the case with Window Active and Window Searching), I had to rely on the anti-spyware programs (Ad-aware and SpyBot Search & Destroy) to identify the program as Apropos Media. While the name "Apropos" does not appear anywhere in the AdIntelligence license agreement or privacy policy, the privacy policy's discussion of the "AdIntelligence AdServer" software does seem to cover what the anti-spyware programs labeled Apropos Media. Moreover, the Apropos Media web site also indicates its association with AdIntelligence (<http://www.apropos-media.com/>). Similar problems hindered my efforts to identify several of the other installed programs as well.

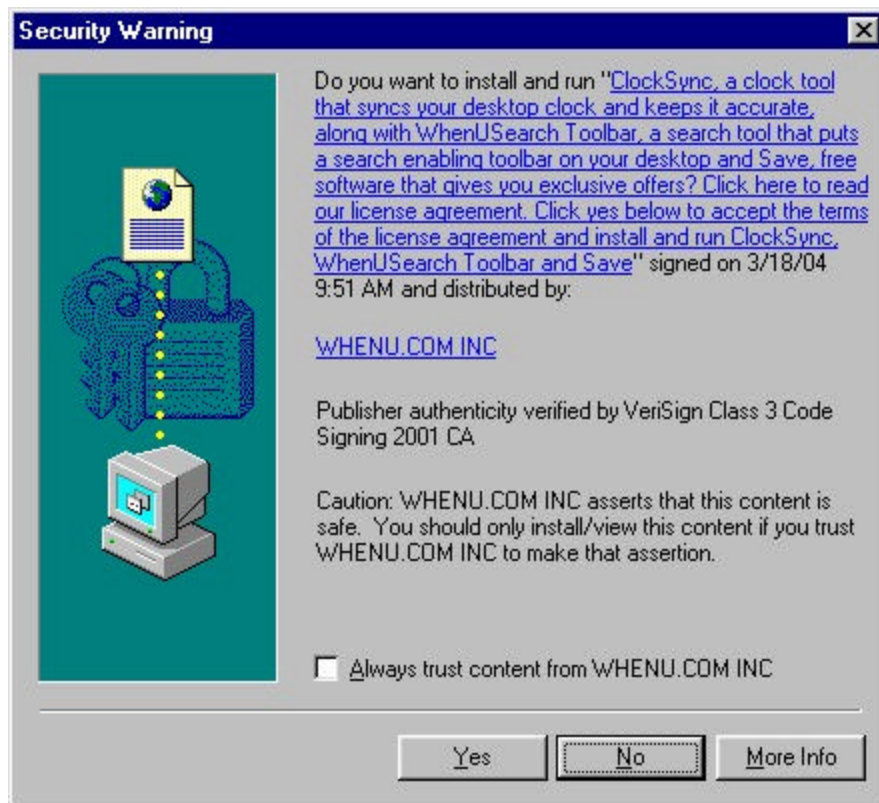
When software vendors dump such a confusing mix of programs and files on users' hard drives and then slap consumers with eighteen pages of dense legalese to explain the resulting mess, those consumers have very little choice but to take vendors at their word -- the chances that they could ever verify that vendors are abiding by the terms of the license agreements are slim to none. Consumers who are faced with such business practices simply cannot be expected to make informed decisions and choices about the software they encounter on the internet.

I should also note at this point that I performed this "drive-by-download" process at LyricsDomain twice on Mar. 24 and once again on Mar. 26 in order to verify my results (I initially visited the site on Mar. 23 to confirm its association with C2 Media). In between installations I completely cleaned up the system, using a combination of vendor-supplied uninstallers, anti-spyware programs, and a manual process of searching for and removing leftover files and directories. The results for this "drive-by-download" process were the same each time I went through it.

This "drive-by-download" was quite similar to many others that I have witnessed. While not all programs installed via this kind of automated installation process bundle so many other third-party programs, many of them do. And the poor quality of information that we saw at the beginning of the installation process is a problem with almost of all these "drive-by-

downloading" advertising programs, which simply do not give consumers the information they need to make an informed decision.

Occasionally consumers do get more helpful information at the start of the "drive-by-download" process for auto-installing ActiveX controls. The problem, however, is that it is currently up to the vendors themselves to determine just how much information consumers receive and how good that information is. Compared with the vague name of the "Software Plugin" (see Figure 2 above) installed in this example on my PC, the description supplied in the ActiveX "Security Warning" box (shown in Figure 7 below) for one of WhenU.com's programs is certainly an improvement:



*Figure 7: "Security Warning" for "ClockSync"*

Some vendors even link to the program's EULA from the "Security Warning" box, as indeed WhenU.com does with this warning box for ClockSync.

All too many vendors do not provide that kind of information, however. Others exploit known security holes in Microsoft's software to bypass the "Security Warning" box entirely. Still worse, if users have lowered the security settings in the Internet zone of Internet Explorer, they will not even see this warning box -- they will simply be surprised at the mysterious appearance of new programs on their PCs. As we shall see in the next section, that surprise could be an extremely unpleasant one, given what these advertising programs can do to consumers' PCs.

## The Aftermath

The eight programs installed on my PC made numerous changes and additions to the system, some more visible and noticeable than others. In this short section I summarize the most obvious or visible changes and additions that resulted. It should be noted that this software was installed and running on my system for less than half an hour. Consequently, there may be other effects of these programs that would become apparent only after weeks or months after installation and which I cannot describe or account for here. Also, I did not attempt to do any packet sniffing or other network forensics, so I cannot describe or account for network connections established by these software programs or the data packets they transmitted to other entities on the internet.

### Toolbars

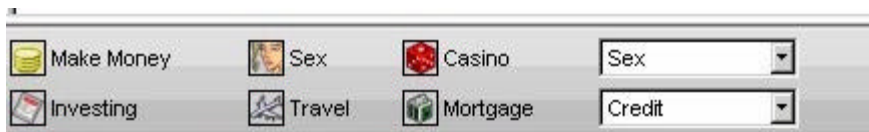
The first and most obvious change to my system was the addition of not one, but three different toolbars by C2 Media's Window Active, Window Searching, and ErrorOnce programs.



*Figure 8: Toolbar # 1*



*Figure 9: Toolbar # 2*

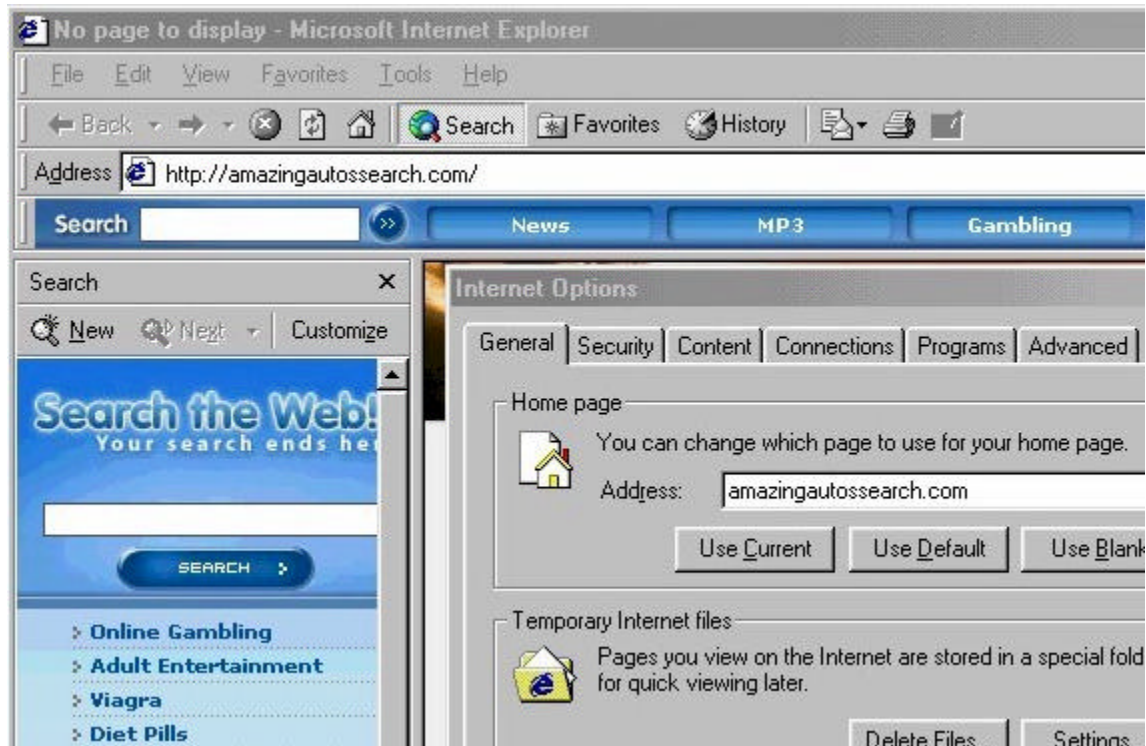


*Figure 10: Toolbar # 3*

Toolbar # 1 was the first to appear, and it popped up right on the desktop. A floating toolbar, it was constantly in the way, even after I closed my browser. Toolbar # 2 appeared within Internet Explorer right under the address bar. I could right-click on it and deselect it from the list of visible Internet Explorer bars to make it disappear, but it would reappear the next time I opened Internet Explorer. Toolbar # 3 appeared towards the bottom of my desktop, as if attached to the taskbar. It appeared only when Internet Explorer was open, though. C2 Media assigns these toolbars different names (Accessory Toolbar, Desktop Toolbar, Pass-Through Toolbar), though which is which I cannot say. Moreover, why it is necessary to have three toolbars, all with apparently overlapping functionality, is a mystery. I did not use any of these toolbars so I cannot report on their actual functionality or other characteristics. Suffice it to say, they were a major annoyance simply because of the screen space they wasted.

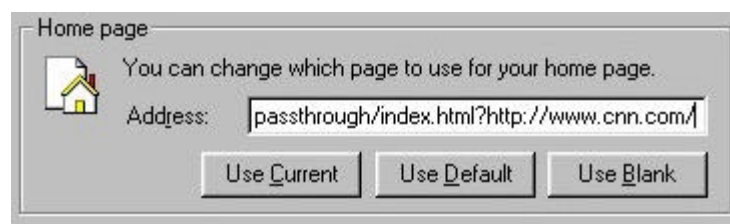
### ***Browser & Desktop Modifications***

C2 Media's programs made other modifications to my browser, however. Most significantly, its software reset my default home page from [cnn.com](http://cnn.com) to [amazingautossearch.com](http://amazingautossearch.com), another site associated with C2 Media. It also reset the default search engine preferences to [amazingautossearch.com](http://amazingautossearch.com) so that every search I did directly through the browser itself (as opposed to visiting a search site like Google) would be sent through C2 Media. Figure 11 shows Internet Explorer with the Internet Options box open (note the default home page) and the search bar opened on the left to the [amazingautossearch.com](http://amazingautossearch.com) search page.



***Figure 11: Hijacked Home Page and Search Bar***

After I attempted to restore my home page to [cnn.com](http://cnn.com), C2 Media's software reset my home page yet again to re-route access to it through [amazingautossearch.com/passthrough](http://amazingautossearch.com/passthrough), which acted as a kind of re-direct or proxy. Figure 12 shows my default home page after I attempted to change it:



***Figure 12: Passthrough Home Page Hijack***

I did not attempt to restore any of my search preferences.

C2 Media also added scads of new "favorites" to my Favorites folder, leading off each of its new folder names with a blank space to ensure that they appeared at the top of my Favorites list:



*Figure 13: New Favorites*



*Figure 14: New Desktop Icons*

Finally, C2 Media's software dropped a number of new icons or internet shortcuts on my desktop for online sites and services. Somewhat less annoying than the three toolbars, the new Favorites and desktop icons were, nonetheless, useless clutter.

### *Dialog Box Advertisements*

One other annoying addition to my system was an advert bar at the bottom of common Windows dialog boxes, presumably so that were I ever in the middle of saving a file or printing a document and found myself suddenly overcome with the spontaneous urge to buy something or enter a sweepstakes contest, I could do so quickly and effortlessly.

This particular system modification was the handiwork of the Alset HelpExpress program. As with the toolbars from C2 Media, I did not use this feature and thus cannot comment on its functionality.



*Figure 15: Alset HelpExpress Dialog Ad*

### ***Pop-ups, Pop-ups, Pop-ups***

All three software vendors warned in their license agreements that their applications would serve pop-ups and other forms of advertising (see Table 1 above), and indeed there was no shortage of pop-ups for me to close. With programs from three vendors running in the background and serving up pop-up advertising, it was almost impossible to tell which program was responsible for any given pop-up, though their frequency seemed to increase as I visited more and more web pages. At one point in my brief experience with this collection of software, I was closing pop-ups every five to ten seconds, and sometimes multiple pop-ups at a go. Web surfing speed also declined, presumably because there were so many programs exchanging data with external network entities (uploading information, downloading advertisements) and consuming bandwidth. I even experienced random browser crashes, undoubtedly because of the sheer number of pop-ups, toolbars, and programs clamoring for attention on my system.

If the license agreements are to be believed, much of this advertising is tied to the monitoring of "computer usage and web surfing behavior" (AdIntelligence Privacy Statement) which is then reported to vendors for the purposes of still further targeted advertising. Again, I did no packet sniffing and kept the software installed for less than half an hour, so I cannot comment on the performance of this advertising software over the course of days, weeks, or months. Suffice it to say that the proliferation of advertising on my desktop made the PC nearly unusable.

### ***Other Programs / Summary***

Several programs installed on my PC had no immediate, visible effects on the system. In particular, the AutoUpdate program from AdIntelligence and the mysterious Rads01.Quadrogram were "silent," yet both were configured to execute on Windows startup and could be found running in the task list. The AutoUpdate program likely updates the AdIntelligence software, though I never saw it do so. Just what Rads01.Quadrogram was doing is not clear; its functionality may have become apparent had I kept it installed for longer than I did, however.

Compared with what other unwanted spyware does to users' PCs, the garbage dropped on my PC was fairly tame, if extremely annoying because it interfered with the usability of the PC. Nastier varieties of spyware can do much worse, however. Some silently install porn dialers that run up users' phone bills into the hundreds and thousands of dollars by connecting to "premium rate" 900 numbers, usually in the former Soviet Union. Still other spyware is known to cause severe system instability and crashes or even break users' Internet connections. Even browser hijacking can be more aggressive than that seen in this example. Some "hijackware" completely locks users out of key browser settings and redirects every search to porn sites. At the extreme edges of the class of software known as "spyware" (where it bleeds into more traditional malware) lie applications that do still more dangerous and destructive things to users' systems.

The vendors responsible for this software prefer to call their software "advertising software," and in that they are not being inaccurate. It is difficult to imagine, though, that most average consumers would knowingly and willingly submit to the aggressive advertising inflicted by this package of programs on a day-to-day basis. However they manage to get this software on their systems, users face a difficult task removing it, as we shall see next.

## The Cleanup

As we saw earlier ("The Installation") the process of installing this collection of advertising programs was fairly simple, provided we didn't ask too many questions or demand readable, straightforward descriptions of the software. The process of removing this software, by contrast, was quite difficult and time-consuming. Although there were vendor-supplied uninstallers for most of the programs, they were not always easy to find. Moreover, most of them didn't work completely. To remove this advertising software completely, I had to use three different anti-spyware programs (SpyBot Search & Destroy, Ad-aware, HijackThis!). At the end of the entire process I still had some minor cleanup work to do by hand.

The complete uninstallation process that I used can be divided into four stages:

1. Run vendor-supplied uninstallers already on the system (from Add/Remove Programs or installation directories)
2. Obtain vendor-supplied uninstallers from web sites and run them
3. Run anti-spyware programs (SpyBot Search & Destroy, Ad-aware, HijackThis!)
4. Perform manual cleanup (remove remaining files/directories by hand)

Readers should bear in mind that I went into this uninstallation process well-prepared. Not only did I know what to look for, but I had taken careful notes during the installation process. I had read the license agreements and noted key URLs and company names. Thus, I knew the programs that had been installed and the web sites to visit to find vendor-supplied uninstallers. Moreover, I had good anti-spyware tools at hand and was experienced in using them. I also had recourse to anti-spyware web sites to get key information about files, directories, and Registry keys. Finally, I am an experienced user of Windows PCs. Thus, I am familiar with the directory structure on Windows PCs as well as the process for editing the Windows Registry.

In sum, I had a number of advantages going into this uninstallation and removal process. Most average consumers and users would enjoy none of these advantages. After recovering from their initial bewilderment at the scads of new programs, pop-ups, and other detritus dropped on their PCs, most consumers would face a long, difficult journey to remove that unwanted software and restore their PCs to a usable state.

### *1. Run vendor-supplied uninstallers already on the system*

Vendors of advertising software tout the uninstallers they provide for their programs. In fact, some vendors even include clauses in their EULAs prohibiting consumers from using third-party tools (read: anti-spyware applications) to remove or uninstall their programs. So I decided to start with the vendor-supplied uninstallers that I could find on my PC. Not all of the programs had left uninstallers on my PC during the installation process, however, so the next step was to track down other uninstallers on vendor web sites and run.



Table 3 below summarizes the programs installed on the PC, what kinds of vendor-supplied uninstallers were available, and how well those uninstallers worked.

<b>Company</b>	<b>Program</b>	<b>Uninstaller Source</b>	<b>Result</b>
C2 Media	Window Active	Add/Remove Programs web site ( x 2)	Partial Partial
C2 Media	Window Searching	Add/Remove Programs	Full
C2 Media	ErrorOnce	<i>uninstalled by Window Active</i>	Full
AdIntelligence	Apropos Media	installation directory	Full
AdIntelligence	AutoUpdate	<i>uninstalled by Window Searching</i>	Partial
Alset	HelpExpress	Add/Remove Programs web site	Fail Fail
Alset	Coupons and Offers	Add/Remove Programs	Partial
???	Rads01.Quadrogram	<i>n/a - uninstalled by ??</i>	Partial

**Table 3: Vendor-Supplied Uninstallers**

The Add/Remove Programs Control Panel applet contained entries for only four programs that had been installed by these vendors: Window Active, Window Searching, HelpExpress, and Coupons and Offers. Of course, to use those uninstallers, one must recognize the entries for what they are. I happened to be very familiar with what was already installed on my PC, so this was not a problem. Other less experienced users might have difficulty identifying the Add/Remove Program entries to remove, especially given the generic names used by some of these programs and the fact that several of the programs' names were never clearly announced during the installation process.

Only one of the uninstallers invoked from Add/Remove Programs worked completely: that for Window Searching. It removed the associated files and Registry keys as well as the desktop icons and favorites. By contrast, the Window Active uninstaller removed critical Registry keys to disable the program, but it left most of the files on the hard drive. It did manage to completely remove the dependent program ErrorOnce, however. The Coupons and Offers uninstaller performed similarly, disabling the program yet leaving files on the drive. The HelpExpress uninstaller failed almost completely -- though it reported success -- leaving behind the files and Registry keys that would allow the program to live another day.

The AproposMedia program from AdIntelligence included an uninstaller program in its installation directory. Many users would never find it, however, even though it is mentioned on the "AdIntelligence Uninstallation Instructions" page (<http://www.adintelligence.net/support/uninstall.html>). When I ran this uninstaller it completely removed AproposMedia program.

Finally, the Window Searching uninstaller that I ran invoked an uninstaller for AutoUpdate that had been put in C:\Windows\System during installation. This AutoUpdate uninstaller performed successfully, though the uninstaller itself was left behind.

All in all, the vendor-supplied uninstallers already on my PC turned in a less than satisfactory performance, so I headed off to vendor web sites to find uninstallers that might finish the job.

## 2. Obtain and run vendor-supplied uninstallers from web sites

I found uninstallers for the C2 Media products on the amazingautossearch.com "Help" page (<http://amazingautossearch.com/help.html>). That page offered two uninstallers -- toolbar\_uninstall.exe and new\_uninstall.exe -- so I grabbed them both. Neither of these uninstallers completely removed the remnants of C2 Media's programs, though they came close: the Window Active directory was completely removed. A few stray Registry keys remained, however, as did the original stub installer download.mp3.exe (in C:\Windows\Downloaded Program Files).

I had some difficulty locating the page for Alset. Although the license agreement mentioned the company's name, it supplied no URL. It took a search on Google to locate the company's home page. The Alset FAQ page (<http://www.alset.com/support.htm>) did indeed have an uninstaller, but it was for "Attune" (RemoveAttune.exe), an older version of HelpExpress. There was no uninstaller for Coupons and Offers that I could find. The "Attune" uninstaller did the same as the Add/Remove Programs uninstaller for HelpExpress: it reported success even though it left all the key files and Registry keys in place.

At this point I still had a number of files on my hard drive from partially uninstalled programs as well as several programs that had been left mostly intact. My next step was to run several anti-spyware programs.

## 3. Run anti-spyware programs

I first ran SpyBot Search & Destroy 1.3 beta 6, a well-regarded and free anti-spyware utility from PepiMK. With the latest available definitions (4 Mar. 2004), SpyBot Search & Destroy flagged several problems on my PC, all of which were related to the software installed in this example "drive-by-download."

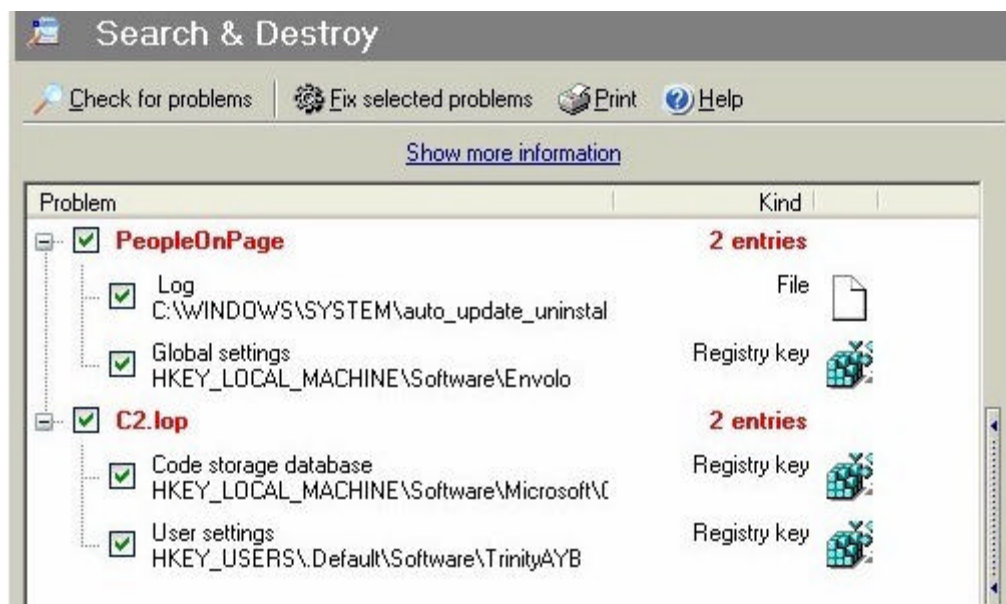
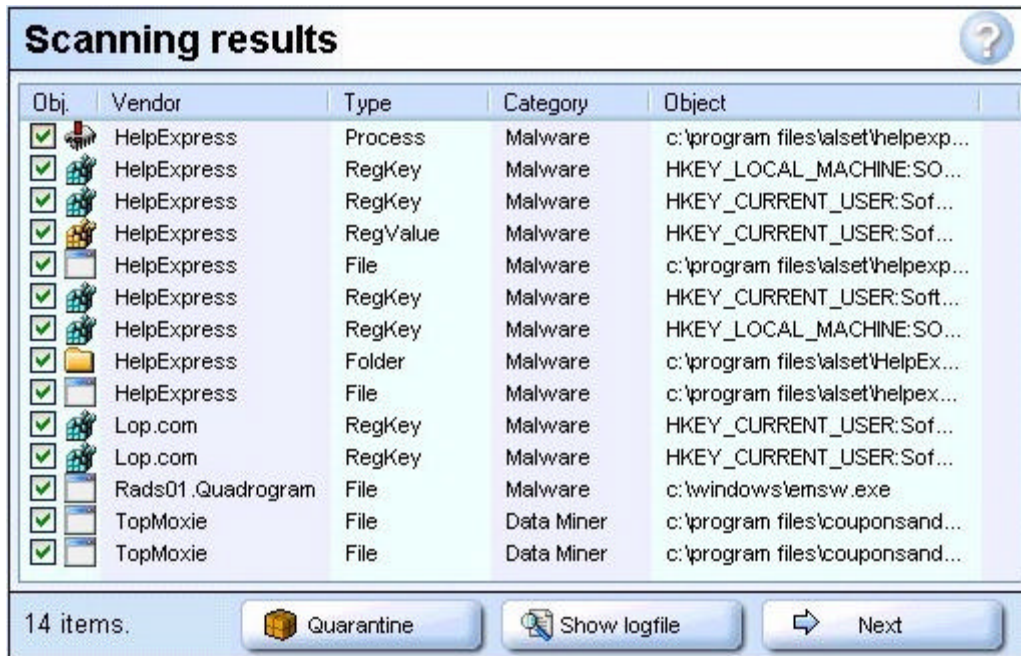


Figure 16: SpyBot Search & Destroy scan results

The "C2.lop" and "PeopleOnPage" entries are files or Registry entries left behind on my system by the vendor-supplied uninstallers. (PeopleOnPage is in fact AdIntelligence.) While none of these entries represented serious problems, they had to go. I let SpyBot fix every problem it identified.

Next I scanned my system with Ad-aware 6.0 Professional build 181, an enhanced for-pay version of Lavasoft's well-known freeware offering, Ad-aware 6.0 Personal. With the latest available reference file (01R274 23.03.2004), Ad-aware found still more problems on my system:



Obj.	Vendor	Type	Category	Object
✓	HelpExpress	Process	Malware	c:\program files\alset\helpexp...
✓	HelpExpress	RegKey	Malware	HKEY_LOCAL_MACHINE:SO...
✓	HelpExpress	RegKey	Malware	HKEY_CURRENT_USER:Sof...
✓	HelpExpress	RegValue	Malware	HKEY_CURRENT_USER:Sof...
✓	HelpExpress	File	Malware	c:\program files\alset\helpexp...
✓	HelpExpress	RegKey	Malware	HKEY_CURRENT_USER:Sof...
✓	HelpExpress	RegKey	Malware	HKEY_LOCAL_MACHINE:SO...
✓	HelpExpress	Folder	Malware	c:\program files\alset\HelpEx...
✓	HelpExpress	File	Malware	c:\program files\alset\helpexp...
✓	Lop.com	RegKey	Malware	HKEY_CURRENT_USER:Sof...
✓	Lop.com	RegKey	Malware	HKEY_CURRENT_USER:Sof...
✓	Rads01.Quadrogram	File	Malware	c:\windows\emsw.exe
✓	TopMoxie	File	Data Miner	c:\program files\couponsand...
✓	TopMoxie	File	Data Miner	c:\program files\couponsand...

14 items.    Quarantine    Show logfile    Next

*Figure 17: Ad-aware "Scanning results"*

Ad-aware found the files and Registry keys for Alset HelpExpress, which had been left substantially intact by the Alset uninstallers I had run earlier. It also found some leftover files from Coupons and Offers (named TopMoxie by Ad-aware) and a few remaining Registry keys for C2 Media's programs. Both Coupons and Offers and the C2 Media programs had already been effectively disabled, however -- what Ad-aware found was just more leftover garbage. Finally, Ad-aware found the Rads01.Quadrogram executable (emsw.exe), which strangely enough was still in the Windows directory. One of the vendor-supplied uninstallers had obviously killed the process for Rads01.Quadrogram and removed the auto-run entry from the Registry (none of the anti-spyware programs found that Registry entry); the executable file had survived, however. As with SpyBot, I let Ad-aware fix every problem it identified.

The third anti-spyware program that I ran was HijackThis! (HJT), a free utility from Merijn which is simple but extremely useful. It logs key system settings that are often modified by spyware applications and allows users to fix those problems. While it is a powerful tool in the

right hands, users must understand what they are looking at in HJT logs -- most of the entries in HJT logs will be normal system configuration settings.

From the log that HJT generated, only two entries were of interest:

```
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =  
http://amazingautossearch.com/searchbar.html
```

```
O2 - BHO: (no name) - {B38EC23A-0D9A-98AC-6F46-1A40DC14B3B0} -  
(no file)
```

The "R1" entry is a search bar hijack left over from C2 Media's software (note that it points Internet Explorer's search bar to amazingautossearch.com). The "O2" entry is for a broken BHO (browser helper object, a kind of plug-in for Internet Explorer) -- the Registry entry is still there for C2 Media's ErrorOnce BHO, however, the file necessary to run that BHO is missing (undoubtedly removed by one of the uninstallers or anti-spyware programs run previously). I used HJT to fix both of these problems.

These anti-spyware programs did a decent job cleaning up after the vendor-supplied uninstallers. Indeed, after my second trial with the "Software Plugin" on Mar. 24, I used the anti-spyware programs first, and they did a significantly better job than the vendor-supplied uninstallers. Nonetheless, no single one of these anti-spyware programs did the job completely. Moreover, there were still a few stray files a directories left on my PC's hard drive.

#### ***4. Perform manual cleanup***

By this point I was completely familiar with the files that had been installed during this "drive-by-download" test, so it wasn't hard to find stray detritus that survived the vendor-supplied uninstallers as well as the anti-spyware programs. There were still some files left over in installation directories for Coupons and Offers and Alset (HelpExpress). An uninstaller for AutoUpdate has been left in C:\Windows\System. Although none of what remained represented a serious problem, it all should have been cleaned up much earlier.

After removing these last few stray files and directories, my PC was finally clean. I rebooted and found it miraculously refreshed, running as it had before the installation of the "Software Plugin" from C2 Media.

## Conclusion

From start to finish this automated "drive-by-download" installation experience was an unpleasant undertaking. Although it began with the fairly innocuous prompt to install the "Software Plugin," it became progressively more difficult and frustrating. The installation process initially provided almost no helpful information about the software to be installed. Key program functionality was then obscured behind an impenetrable wall of legalese, which few consumers would have any hope of understanding. And though a careful review of the license agreements and privacy policies revealed that most of the functionality of the software installed on my PC had in fact been disclosed, the effects of that software on my system were serious inasmuch as the new toolbars and endless advertising interfered with the normal use of the computer. Finally, the job of cleaning up and removing the software proved to be a long and cumbersome process, even for someone who had the experience and tools to do it.

Consumers who encounter the "Software Plugin" at the LyricsDomain web site and mistake it for a simple browser plug-in necessary to use the music content of the site are in for a nasty surprise. After clicking but two buttons -- "Yes" in the "Security Warning" box and "Accept" in the "Verification Box" -- they will be treated to the installation of eight different programs from at least three different vendors. Three new toolbars will be added to their systems. Their browser's home page and search preferences will be hijacked, and they will be inundated with pop-up advertising. So thoroughly does this advertising software penetrate the system, users will be confronted with advertising even when they print documents or save files.

To clean this mess up on my own PC, I had to run four different uninstallers from Add/Remove Programs or program installation directories, only to find that I had to download and run three more uninstallers from vendor web sites. Even then my system was not clean. Three different anti-spyware tools were required to remove most of what was left, including one advertising program that the vendor's uninstallers had simply failed to uninstall. At the end there were still a few stray files and directories left for me to remove by hand.

Compared with what could have happened, however, I got off easy. My internet connection was not broken, and I have no reason to fear the arrival of the next phone bill. My system remained fairly stable, though I did experience a few browser crashes, and system performance took an enormous hit. Moreover, though the removal process proved to be a time consuming chore, I was ultimately able to install and run anti-spyware programs. Despite being somewhat difficult to remove, the advertising software did not deliberately undermine my removal efforts or sabotage my system, as other unwanted spyware is known to do.

Nonetheless, this example "drive-by-download" should illustrate the enormous difficulties that consumers face when they encounter apparently innocuous software that is presented to them in misleading and confusing contexts. Not surprisingly, they are complaining, and we would do well to understand the reasons for those complaints and take action to solve the problem.

## More Information

For more information on the software discussed in this document, see the following sources:

### *Anti-Spyware Programs*

#### **Ad-aware**

- <http://www.lavasoft.de/>
- <http://www.lavasoftusa.com/>

#### **SpyBot Search & Destroy**

- <http://beam.to/spybotsd>
- <http://spybot.safer-networking.de/>

#### **HijackThis!**

- <http://www.spywareinfo.com/~merijn/>
- <http://www.spywareinfo.com/~merijn/htlogtutorial.html> (tutorial)

### *Advertising Software Programs*

#### **AdIntelligence / Apropos Media**

- <http://www.adintelligence.net/> (AdIntelligence home page)
- <http://www.apropos-media.com/> (Apropos Media home page)
- <http://www.peopleonpage.com/> (PeopleOnPage home page)
- <http://www.doxdesk.com/parasite/AproposMedia.html> (doxdesk.com information)
- [http://www.spywareguide.com/product\\_show.php?id=625](http://www.spywareguide.com/product_show.php?id=625) (SpywareGuide.com information)

#### **Alset HelpExpress**

- <http://www.aset.com/> (home page)
- <http://www.kephyr.com/spywarescanner/library/helpexpress/index.phtml> (Kephyr.com information)
- <http://www.c-squad.org/hxdl.html> (CSquad.com information)
- <http://www.pestpatrol.com/PestInfo/h/helpexpress.asp> (Pest Patrol information)

#### **C2 Media / Lop.com**

- <http://www.lop.com/> (home page)
- <http://amazingautossearch.com/> (home page)
- <http://www.doxdesk.com/parasite/lop.html> (doxdesk.com information)
- <http://www.spywareinfo.com/articles/lop/> (SpywareInfo.com information)

#### **Rads01.Quadrogram / "Peper" trojan**

- <http://www.kephyr.com/spywarescanner/library/peper Trojan/index.phtml> (Kephyr.com information)
- [http://vil.nai.com/vil/content/v\\_100635.htm](http://vil.nai.com/vil/content/v_100635.htm) (Network Associates information)