

# **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."

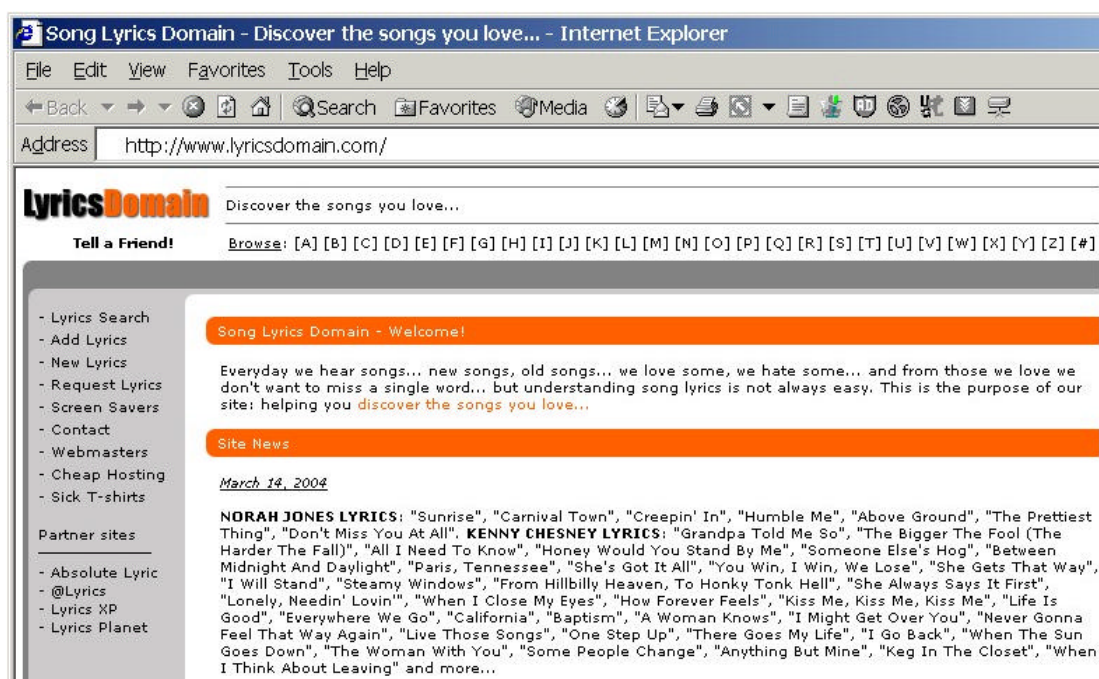
For this example "drive-by-download" I used an old, custom-built Pentium 166 PC with 64 mb RAM. It was loaded with Windows 98 SE and Internet Explorer 5.5 w/ SP2. Although this system is fairly dated in comparison with the systems now being sold by major OEMs, it is still quite usable. I deliberately 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*

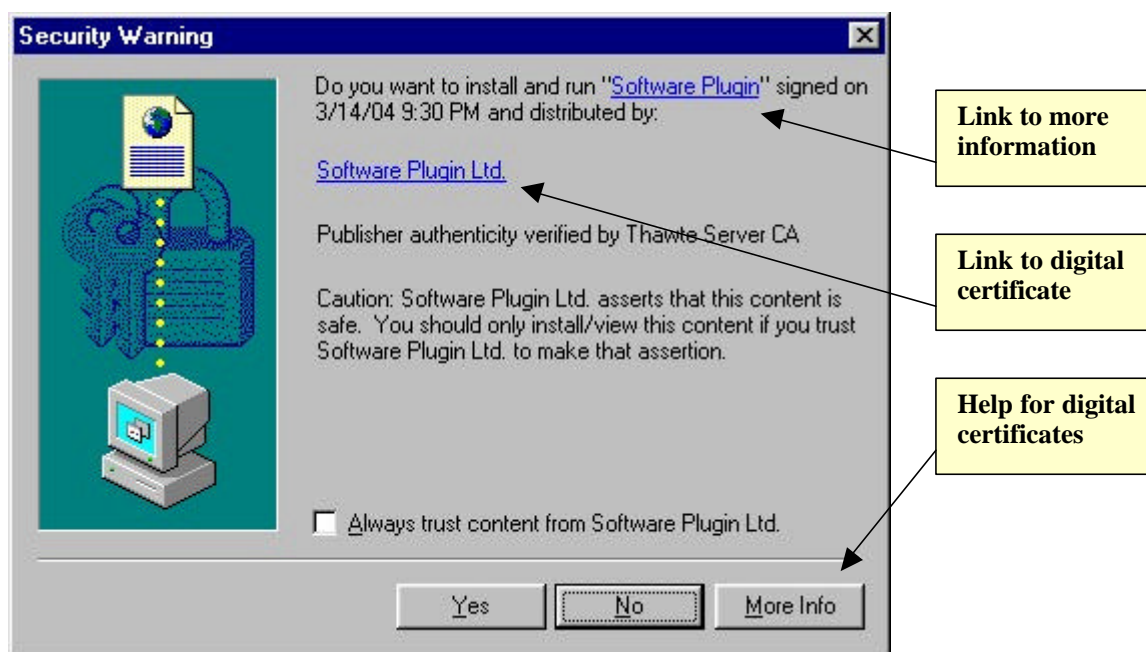
The site's privacy policy (<http://www.lyricsdomain.com/privacy.html>) is fairly innocuous and even appears to be "consumer friendly":

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 was familiar with lyricsdomain.com and the software that I would encounter there, many consumers would 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 little 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



provides only a help page (see Figure 5 below) 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."

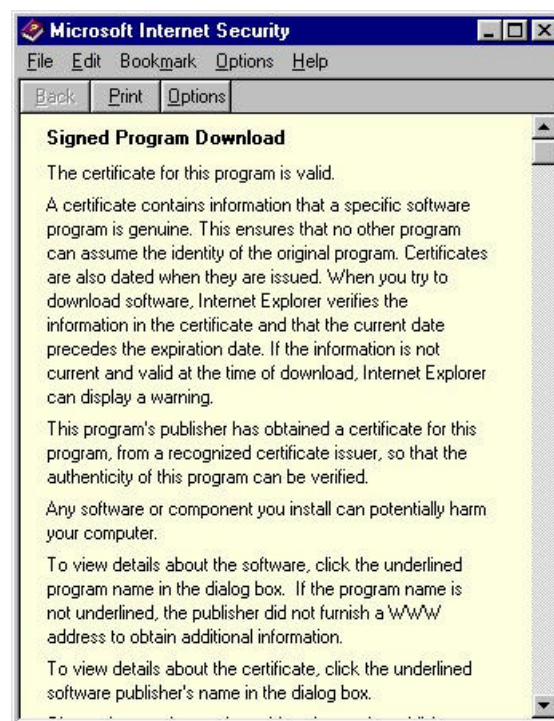


Figure 5: "More Info"

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."

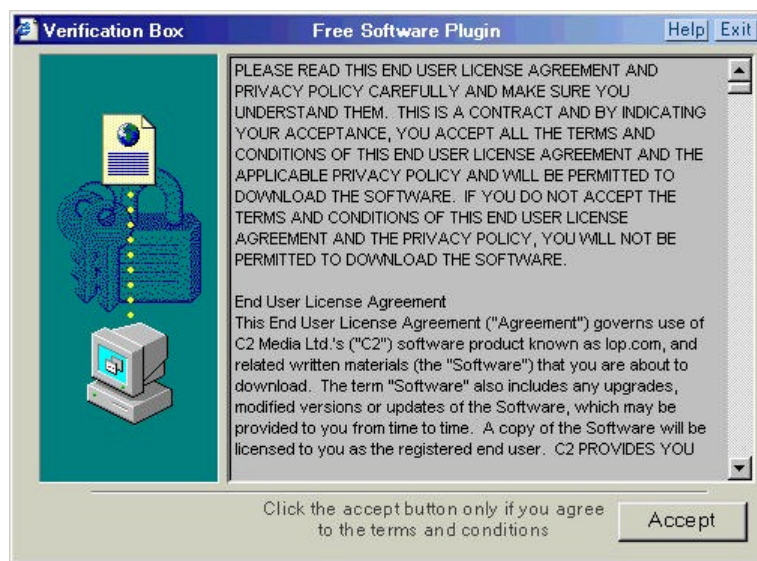


Figure 6: "Verification Box - Free Software Plugin"

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/ popunders)</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.

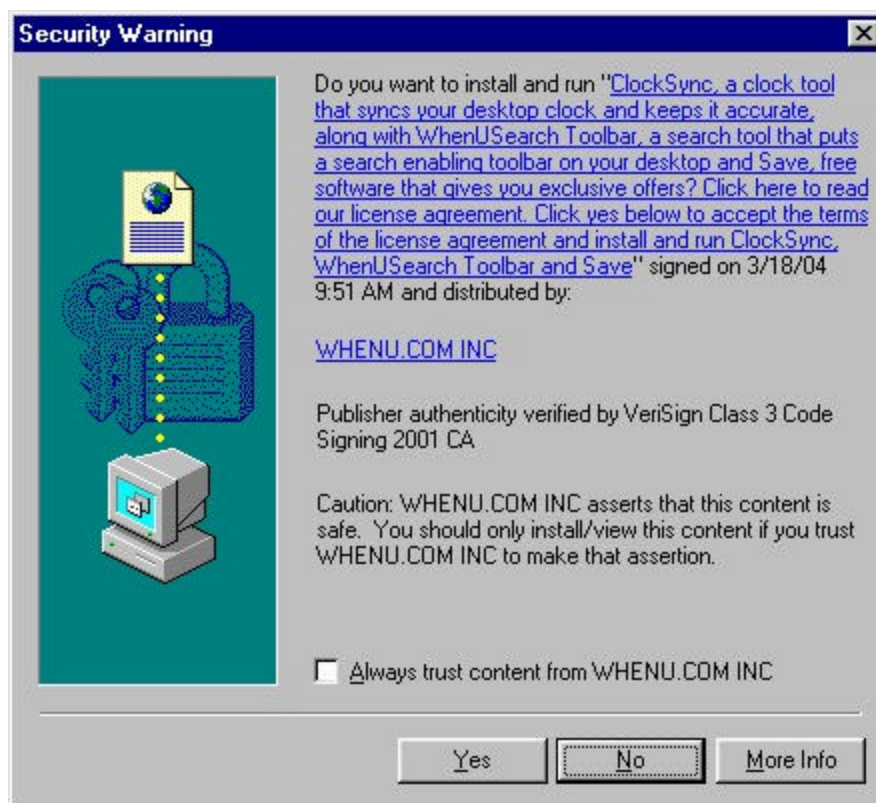
I should also note at this point that I performed this "drive-by-download" process at LyricsDomain twice on Mar. 24 and once again on Mar. 26 in order to verify my results (I initially visited the site on Mar. 23 to confirm its association with C2 Media). In between installations I completely cleaned 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 left to 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 weeks or months after installation and which I cannot describe or account for here. Also, I did not perform 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*

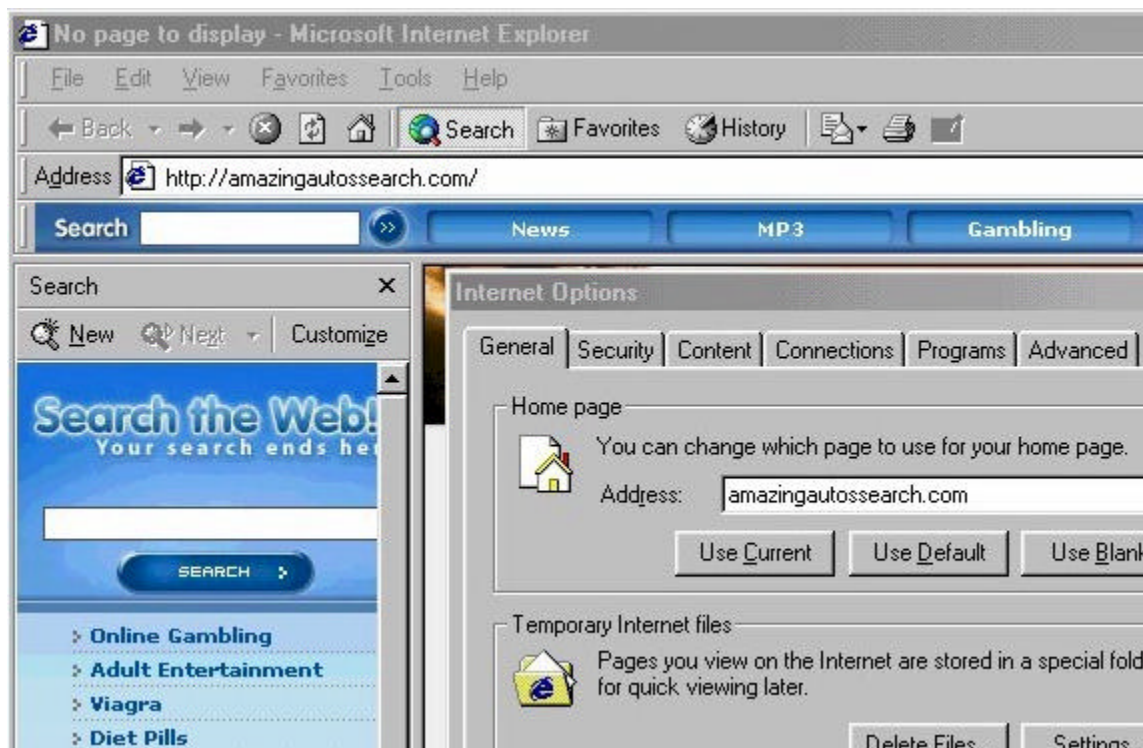


*Figure 10: Toolbar # 3*

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.

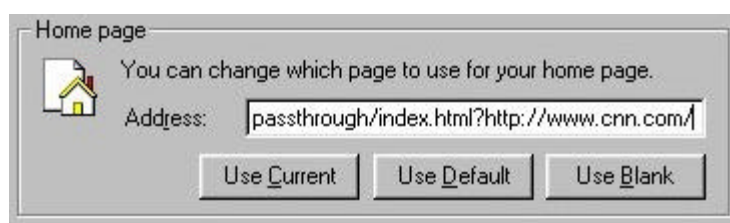
## ***Browser & Desktop Modifications***

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:



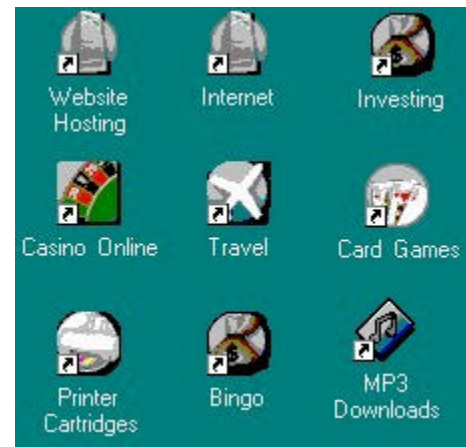
***Figure 12: Passthrough Home Page Hijack***

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 (see Figure 16 below), all of which were related to the software installed in this example "drive-by-download."

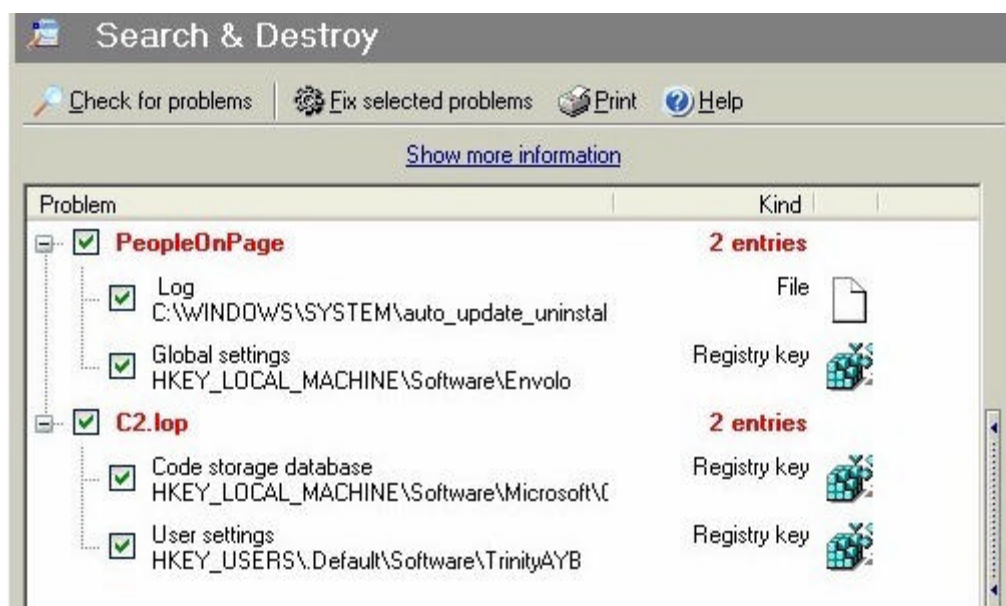
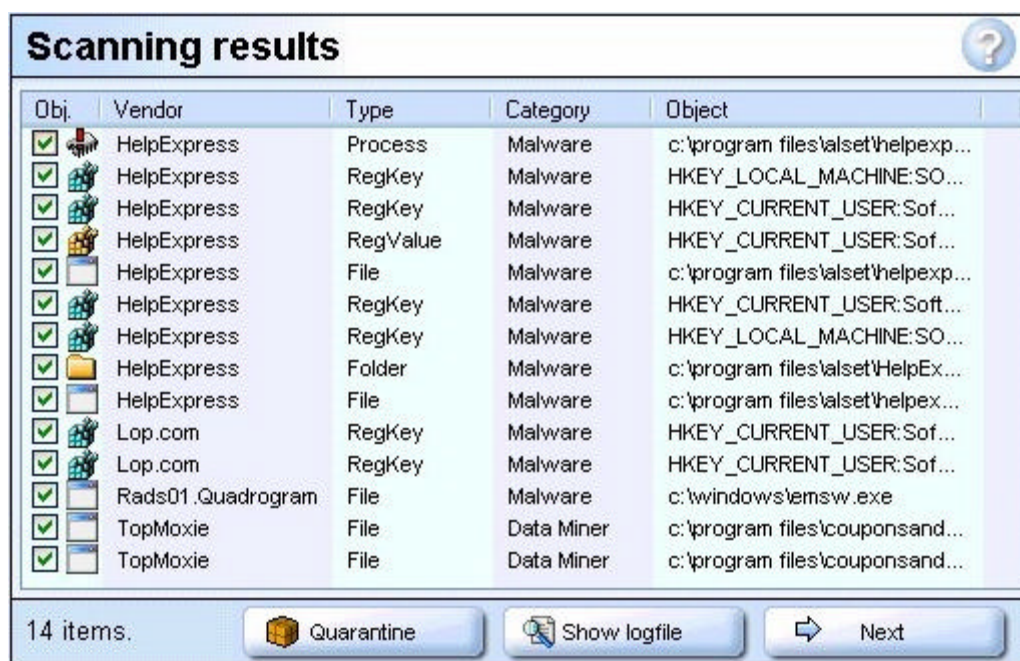


Figure 16: SpyBot Search & Destroy scan results

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:Soft...
✓	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 and 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/pepertrojan/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)