Alleged Improvements to COAST-Certified Versions of 180solutions' Software

Sunbelt Software Spyware Research Center

13 March 2005

Introduction

180solutions is a contextual advertising company that makes and distributes several advertising software applications, including the 180search Assistant (http://180searchassistant.com) and Zango (http://zango.com). Previously it distributed a substantially similar advertising application known as nCase, though the company began phasing out that older software during 2004. All of 180's applications track users' web surfing behavior and open advertising windows on users' desktops based on data collected about users' surfing habits. As a result, 180's software has been widely targeted for detection and removal by anti-spyware programs. (For a thorough summary of the various versions of 180's advertising applications, see Andrew Clover's excellent write-up on "nCase": http://www.doxdesk.com/parasite/nCase.html.)

On January 14, 2005, 180solutions announced that it had been admitted to the Consortium of Anti-Spyware Technology vendors (COAST, coast-info.org). In its press release (http://www.180solutions.com/pages/pressrelease.aspx?node=/Press/COAST) 180solutions claimed that it had been subjected to a "rigorous review" by COAST and that it had worked with COAST to develop new versions of its main advertising applications that adhered to COAST's strict "Code of Ethics and Guidelines":

> In order to join COAST, software developers like 180solutions must pass a rigorous review and agree to adhere to the COAST Code of Ethics and Guidelines including ongoing, frequent reviews to ensure continued compliance. As a result of being accepted for membership, 180solutions is now releasing versions of its applications that have been reviewed and evaluated by COAST and found to meet COAST standards. The company has begun working with its partners to insure all of their channels will transition to distributing only these COAST reviewed versions of its software within the next 90 days.

180solutions began distributing these new COAST-certified versions of the 180search Assistant and Zango in the days and months after its admission into COAST. These new versions sport a new tray icon, a revamped uninstaller, and a "CBC Force prompt" for notice and disclosure during installation. Trey Barnes, executive director of COAST, characterized these new versions of 180's software as "spyware-free" and lauded 180solutions for "making substantial modifications to its software, and working with channel partners to distribute only the modified versions of its products in the future" (http://www.180solutions.com/pages/pressrelease.aspx?node=/Press/COAST).

Given the functionality of 180solutions' software as well as its checkered distribution history -- a history which includes rampant "force-installs" of 180's software on users' PCs without those users' full knowledge and consent -- the anti-spyware community is entirely justified in being skeptical of 180's claims to have reformed its software and distribution practices. In February 2005 Sunbelt Software, makers of the CounterSpy anti-spyware application, began looking into these new versions of 180solutions' software as well as 180solutions' representations concerning their alleged improvements.

This white paper examines the changes made in the new COAST-certified versions of the 180search Assistant and Zango. Contrary to the claims made by 180solutions and COAST, this white paper concludes that the changes made to 180's software do not constitute substantial

improvements and are largely inadequate to improving users' experiences with 180solutions' software. Still further, this paper documents the apparent ongoing attempts by 180solutions itself to bypass its new "CBC Force prompt" so as to continue updating, servicing, maintaining, and deriving economic benefit from installations of its software that 180solutions must surely know are the products of illegal "force-installs" on users' PCs. The implications of this serious behavior are then discussed.

Contents

Introduction 1

Background: Problems w/ 180solutions' Software 3
- Poor Installation Practices 3
- "Force-installs" 5
- Windows Media installs 6
- Rogue distributors 8
- Updates to 180solutions' software installations 9

Alleged Improvements to 180solutions' Software 11
- Advertising 11
- Data collection, transmission, & sharing 13
- Uninstallers 15
- Tray icon 18
- "CBC Force prompt" 18

Conclusion 26

References 27

About Sunbelt Software 28

Background: Problems w/ 180solutions' Software

Before addressing the changes made in the new COAST-certified versions of 180solutions' advertising applications, it is important to summarize the problems with older versions of 180's software, for 180solutions and COAST specifically claim that the revamped 180search Assistant and Zango applications are designed to remedy those problems.

Poor Installation Practices

180solutions' advertising applications have been distributed through a variety of methods, including automated, browser-based installations at third-party web sites, bundled installs through "freeware" and "shareware" applications, and traditional setup executables downloadable from 180solutions' own web sites. Many if not most of these distribution methods have seen 180's software installed on users' PCs without providing users clear, conspicuous notice, disclosure, and choice and without gaining their full, meaningful knowledge and consent.

Online, browser-based installations

180solutions' software has been distributed via automated, browser-based installation processes (*i.e.*, "ActiveX installs") at a variety of third-party web sites. In many cases the software is presented to users alone or by itself, being identified as "nCase" or the "180search Assistant" from "180Solutions" in the ActiveX Security Warning box that opens when users land on web pages that initiate the installation of the software.

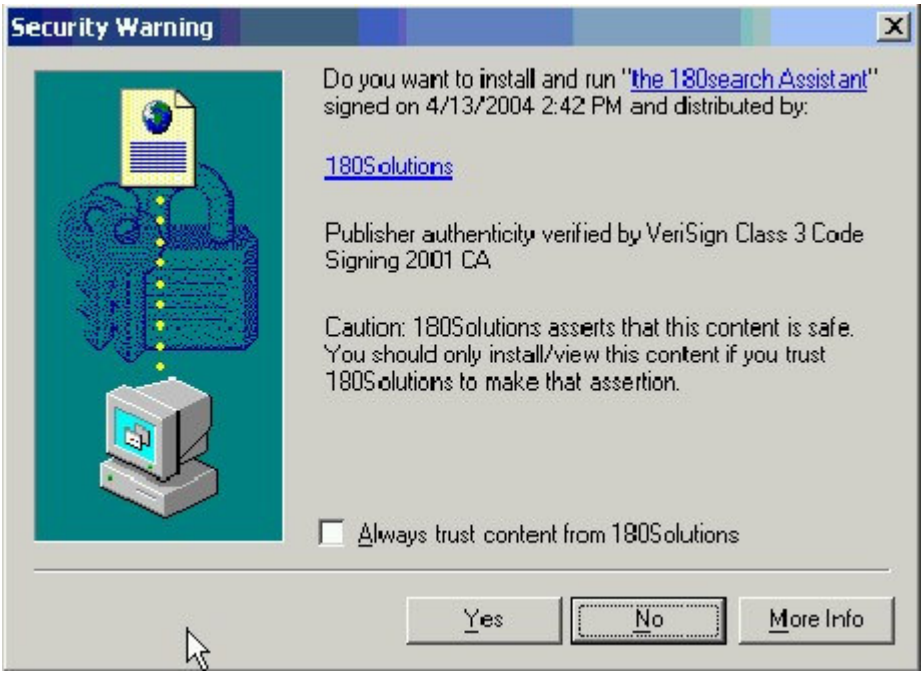

Figure 1: "Security Warning: 180Solutions"

In other cases, though, 180's software has been distributed as part of a bundle of applications that are installed through such ActiveX installation processes. In one such installation encountered during Sunbelt's testing in early March 2005, for example, the 180search Assistant was bundled with the "IE-Plugin," "Bargain Buddy," "ClipGenie," and Midaddle" "adware" applications. This installation, launched at the tabpower.com web site, dropped numerous programs on the test PC. In another online installation performed through a Java applet at lyricsdomain.com and other music lyrics sites during early March 2005, the 180search Assistant was installed with "ISTBar," "PowerScan," "Sidefind," "PeopleOnPage," and the "YourSiteBar," though the presence of 180's software was nowhere disclosed prior to installation, making this installation a "force-install."

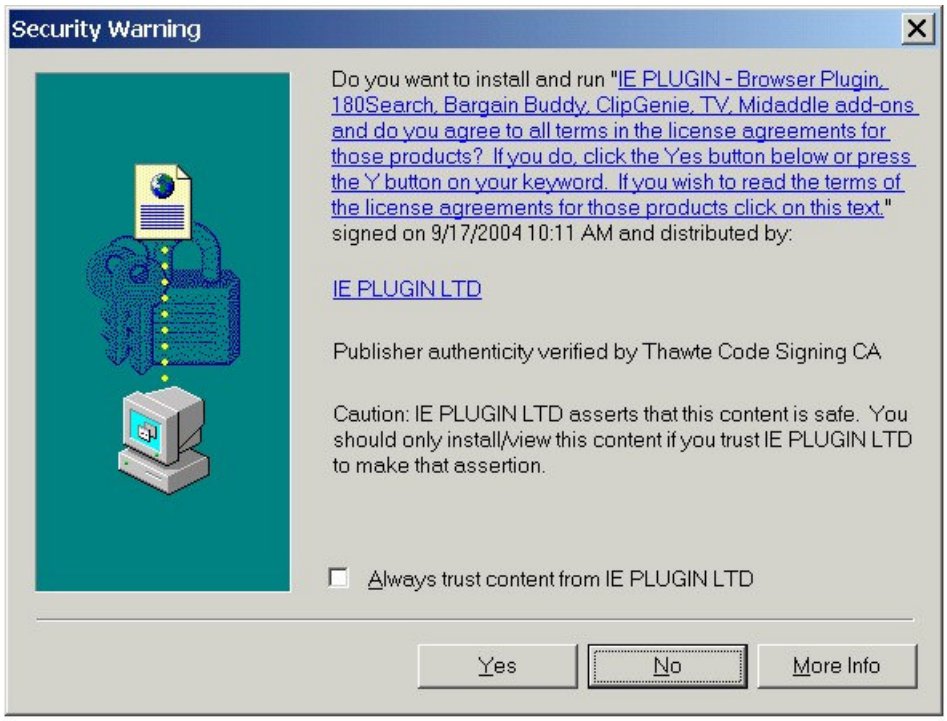

Figure 2: "Security Warning: IE PLUGIN LTD"

Andrew Clover reports that 180's software has been installed with still other "adware" applications including: "FavoriteMan," "BookedSpace," "NeoToolbar," "InternetOptimizer," "Roimoi," and "ISTbar" (http://www.doxdesk.com/parasite/nCase.html). Additionally, Sunbelt has discovered End User License Agreements (EULAs) from SurfAssistant.com, Media-Motor.com, Slotchbar.com, Crackz-Serialz.com, Odysseus Marketing (kazonon.com), and CrazyWinnings.com that disclose the installation of 180solutions' software as part of a package of applications.

Whether these ActiveX installation processes are used to install 180solutions' software alone or as part of a bundled package of "adware" applications, users find these automated, browser-based installations at third-party web sites enormously bewildering and confusing, often mistaking the software to be installed for browser plugins required to view the content of the web sites being visited. When multiple "adware" applications are delivered to the user's desktop via a single ActiveX installation prompt, the confusion and bewilderment is only increased, as most users

will simply not expect that by clicking through a one ActiveX Security Warning box they could be consenting to the installation of multiple "adware" applications. (For a fuller discussion of the problems with automated, browser-based installations of advertising applications see https://netfiles.uiuc.edu/ehowes/www/dbd-anatomy.htm.)

Bundled "freeware" installations

180solutions' software has been bundled with "freeware" or "shareware" applications. In some cases 180solutions' software has been bundled with third-party applications, examples of which include "KiwiAlpha" (http://www.kiwialpha.com/), "MusicHall" (http://www.mymediacenter downloads.com/), and screensavers and wallpapers from Topeleven.net. In such cases the software bundled is the 180search Assistant.

180solutions also distributes advertising-supported "freeware" applications of its own from the Zango.com web site. These applications include, for example, games, desktop add-ons, and Internet programs such as an instant messenger application. In the case of programs distributed via Zango.com, the bundled application is Zango instead of the 180search Assistant, though the functionality of these advertising applications is substantially similar.

Notice, disclosure, choice, & consent

Older versions of 180's software provide poor notice and disclosure even in the best of conditions. Users who install "freeware" that bundles 180's software will get, at best, a EULA, though 180's EULA may appear appended to the end of an already long EULA and Privacy Policy from other software vendors. In some cases, the host EULA and/or Privacy Policy has contained only a URL pointing to 180's EULA, not even the full text of the EULA. Either way, few users are likely to be fully aware of the installation of 180's software in such circumstances.

Automated, browser-based installs offer still less notice and disclosure, as users will be encountering ActiveX "Security Warning" boxes at third-party web sites amidst inherently confusing circumstances. That "Security Warning" box offers precious few clues about the true nature of the software, and many users won't know enough to click the embedded link to read the EULA (which may or may not contain the full text of 180's EULA). In cases where 180's software is being installed as part of a bundle of applications, it is highly likely that users will not notice any mention of 180's software.

"Force-installs"

There is a well-documented history of 180's software being "force-installed" or "stealth-installed" via security exploits, including exploits performed by CoolWebSearch-related (CWS) software and web sites. Andrew Clover notes that 180's software has routinely been installed via "IE security holes exploited by CoolWebSearch" (http://www.doxdesk.com/parasite/nCase.html). Ben Edelman has gone so far as to claim that "N-Case is definitely installed without consumers' informed consent in many or most instances" (http://seattlepi.nwsource.com/business/167416_180folo02.html). In these kinds of cases, users receive absolutely no warning

that 180's software is being installed, and their full, meaningful knowledge and consent is not gained.

Edelman and other researchers documented one prolific example of such force-installs in November and December of 2004, when they reported that a number of CWS-related domains were hosting exploit pages to which unsuspecting users were directed when they visited web sites hosted on web servers that had been compromised with rootkits:

> News: Major Exploit Underway...
> http://www.dslreports.com/forum/remark,11904374~mode=flat
>
> Who Profits from Security Holes? (Ben Edelman)
> http://www.benedelman.org/news/111804-1.html

The up-shot of this exploit process was the "force-installation" of dozens of "adware" programs and porn dialers on users' PCs, including 180solutions' software. Edelman's write-up includes a video of one example exploit process that clearly "force-installs" 180solutions' software. So far as Sunbelt software knows, the web sites and groups involved in those security exploits are still in operation.

Edelman has documented and summarized other less than acceptable installation practices used to drop 180's software on users' desktops:

> 180 Talks a Big Talk, but Doesn't Deliver
> http://www.benedelman.org/news/011705-1.html
>
> 180solutions Installation Methods and License Agreement
> http://www.benedelman.org/spyware/180-affiliates/installation.html#license

As noted earlier, when 180solutions' software is installed as part of a bundle of "adware" applications, the specific presence of 180's software may not be disclosed to the user beforehand, making those particular installations of 180's software "force-installs" or "stealth-installs."

Such force-installs continue to the present point in time. At the time of this writing (early March 2005), Sunbelt has just finished documenting yet another CWS-related exploit performed at 600pics.com that delivers multiple "adware" programs, including the 180search Assistant, as well as porn dialers and even purported "anti-spyware" programs to users' desktops with no warning or notice whatsoever. (Sunbelt possesses archived copies of the files and web pages used in this installation.)

Windows Media installs

As documented in early January 2005 by several researchers and reporters, 180solutions' software has been installed via Windows Media Player files that initiate the installation of "adware" programs when they open hosted instances of Internet Explorer, ostensibly to acquire license information needed to play DRM-protected media files. See:

Adware Installed through WMA Files
http://www.dslreports.com/forum/remark,12245912~mode=flat

Risk Your PC's Health for a Song?
http://www.pcworld.com/news/article/0,aid,119016,00.asp

WMP Adware: A Case Study in Deception
http://www.dslreports.com/forum/remark,12298989~mode=flat~start=0

Media Files that Spread Spyware (Ben Edelman)
http://www.benedelman.org/news/010205-1.html

These installations are especially deceptive because the software is presented to users in confusing circumstances and through methods and means that have been deliberately designed to give the false impression that such software is required to play the media files.

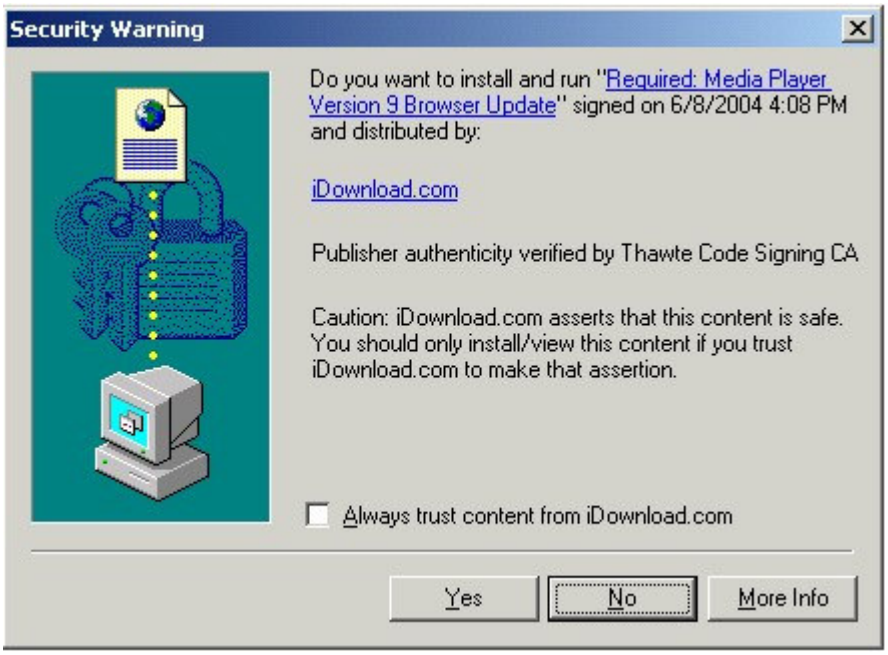

Figure 3: "Security Warning: iDownload.com" (Windows Media Player)

In some instances, the installation of 180solutions' software is not disclosed at all, amounting to a

Figure 4: Windows Media Player "License Acquisition" box

"stealth-install" or "force-install" of the software without the user's permission or consent.

These Windows Media installations are on-going. In mid February 2005, Sunbelt documented a force-install of the 180search Assistant through a DRM-protected Windows Media Player file, raising serious questions about 180's knowledge and control of its software distribution channels.

Rogue distributors

One major and unavoidable source of concern for the anti-spyware community must necessarily be 180's use of pay-per-install affiliate networks to distribute its software. Such networks offer 180 a powerful method for distributing its software via all manner of software and web sites (see http://www.180solutions.com/pages/partners.aspx). The problem, however, has been that 180 seems unable or unwilling to rein in distributors ("partners") who resort to unethical means of presenting 180's software to users and even installing it on users' PCs through security exploits in order to get paid for those installations. Moreover, as Ben Edelman has documented, 180solutions has been unscrupulous in soliciting "partners" to distribute its software, resorting even to unsolicited commercial email (*i.e.*, "spam") to recruit distribution "partners" (http://www.benedelman.org/news/011705-1.html).

As noted earlier, 180solutions' software has a bad history of being "force-installed" on users' PCs. This "force-installation" problem can be directly attributed to 180solutions' poor decisions in selecting distribution "partners," for even if 180solutions might be aware only of the particular "partners" it has selected, those "partners" may themselves recruit others to distribute their software packages that include 180's software. What eventually results is a *de facto* layered network of distributors, only the top layer of which 180 itself directly recruited as "partners."

The problems with these multi-level, pay-per-install affiliate networks were recently highlighted by Ari Schwartz of the Center for Democracy & Technology in his testimony before the House Committee on Energy and Commerce regarding H.R. 29 (the "SPY ACT") on January 26, 2005 (http://www.cdt.org/testimony/20050126schwartz.pdf). The CDT rightly claimed that

> The existence of this complex network of intermediaries exacerbates the spyware problem in several ways. For example:
>
> • Industry Responsibility – Adware companies, advertising brokers, and others all may disclaim responsibility for attacks on users' computers, while encouraging these behaviors through their affiliate schemes and doing little to police the networks of affiliates acting on their behalf. Advertisers, too, should be pushed to take greater responsibility for the companies they advertise with.
>
> • Enforcement – Complex webs of affiliate relationships obstruct law enforcement efforts to track back parties responsible for attacks. The complexity of these cases puts an extreme strain on enforcement agencies, which struggle to tackle the problem with limited resources.
>
> • Consumer Notice – Adware companies and their affiliates have been reluctant to clearly disclose their relationships in a way that is transparent to consumers. Appendix A excerpts a recent CDT submission to the FTC on this issue, demonstrating ways that adware companies could begin to improve transparency in bundling and ad-support arrangements. Companies have resisted these changes. Efforts to bring transparency to the full chain of affiliate and distribution arrangements have met with even greater opposition.

> For these reasons, the affiliate issue has become a central aspect of the spyware epidemic. Finding ways to effectively reform affiliate relationships will remove a lynchpin of spyware purveyors' operations.

180solutions gives every indication of being aware of problems with its distributors, yet seems to want to avoid taking full responsibility for the misuses of its software by portraying itself as the innocent victim of circumstances and powers outside of its control -- as if the distribution problems documented above were unavoidable "acts of nature." In an April 2004 interview with the *Seattle Post-Intelligencer*, Todd Sawicki of 180solutions appeared to acknowledge that 180 was not fully in control of its software distribution channels (http://seattlepi.nwsource.com/business/167416_180folo02.html):

> [Sawicki] said n-Case could get bundled with other free software programs without the company's knowledge. And that could lead to the n-Case software fastening to individual's computers without their knowledge, he said.

In a November 2004 interview with the *L.A. Times*, though, Sawicki went further, characterizing persons performing force-installs of 180's software as "guys in Bermuda, offshore. They're the online equivalent of spammers" (http://www.latimes.com/news/nationworld/nation/la-na-spyware26 nov26,0,7513997.story?coll=la-home-headlines).

The explanations offered by 180solutions are less than convincing, as those rogue affiliates are clearly installing 180's software because they have some expectation of being paid for the installations -- perhaps not directly by 180 itself, but by "middleman" distributors, as documented by the Center for Democracy & Technology. Moreover, this kind of excuse-making does little to inspire confidence in 180's commitment to ending the abuses of its affiliate distributors. Finally, as discussed later in this white paper, 180solutions is silently updating older installations of its software to the latest versions, clearly electing to continue to derive economic benefit from those installations, many if not most of which 180solutions must surely know are the product of illegal "force-installs" or "stealth-installs."

Updates to 180solutions' software installations

In its recent testing of 180solutions' software, Sunbelt encountered a mix of old and new versions of 180's advertising applications. The software versions distributed directly from 180's own web sites (180searchassistant.com and Zango.com) were primarily the new, COAST-certified versions (versions 6.2.3.0, 6.6.3.2, or 6.6.4.0). When encountered in installations from or at third-party web sites, the installed software consisted primarily of the old versions (usually version 5.15.15.0 or earlier).

In some cases, though, these old versions connected to 180's servers, and downloaded and installed the latest version of the software. This auto-update mechanism is disclosed in the EULAs for 180search Assistant and Zango, though it cannot be controlled or disabled by the users. From the 180search Assistant EULA (http://www.180searchassistant.com/eula.html):

> 6. Updates. 180solutions, in its sole discretion, may provide you with released Updates to the Software as part of this Agreement. The Software will check with 180solutions for these Updates automatically,

> and in the event that an Update is available, the Update will be installed automatically by the Software. Nothing herein shall be construed or interpreted as requiring that 180solutions provide these updates.

When older versions of 180's software were updated to the new COAST-certified versions, the file names remained the same, as did the installation directories.

Curiously, not all older versions were updated, though. The Windows Media Player installation of the 180search Assistant mentioned earlier was updated to the new version, as was the 180search Assistant installed via a Java applet at lyricsdomain.com. In other instances, though, the older software was not updated. For example, the installation of the 180search Assistant encountered at tabpower.com was not updated, nor were the versions of 180search Assistant bundled with "MusicHall" or the screensavers and wallpapers from TopEleven.net.

Just why some installations were not fully updated to the latest version of 180search Assistant is not fully understood, though there could be any number of explanations. Clearly, though, 180solutions is silently updating many older installations of its software to the new COAST-certified versions of the 180search Assistant.

Alleged Improvements to 180solutions' Software

180solutions claims that the newer COAST-certified versions of its 180search Assistant and Zango advertising programs incorporate changes that should substantially improve users' experiences with its software and make those applications more privacy-friendly, including:

1. Advertising windows that are clearly labeled as originating from 180solutions
2. Privacy-friendly data collection and transmission practices
3. Uninstallers that do not require an internet connection to work
4. Tray icons that alert users to the presence of 180's software
5. "CBC Force prompts" that ensure notice and disclosure during installation

As we shall see, none of these changes actually represents a substantial improvement to 180solutions' software. Still worse, in one case 180solutions itself appears to be undermining the potential improvements that could have resulted from the changes to its software.

Advertising

The main purpose of 180solutions' software -- whether it be the older nCase software or the newer 180search Assistant and Zango programs -- is to display advertising on the user's desktop based on the web sites visited by the user. 180solutions trumpets the fact that the contextual advertising opened by its software is clearly labeled and easily closed (http://www.180solutions.com/pages/privacypledge.aspx).

The 180search Assistant and Zango EULAs do disclose this advertising functionality. From the 180search Assistant EULA (http://www.180searchassistant.com/eula.html):

> 180search Assistant will periodically direct you to our sponsors' websites. 180search Assistant will collect information about the websites you visit, but will not collect any information that will be used by 180solutions to identify you personally. The information that 180search Assistant collects and transmits to 180solutions will be used to provide you with access to comparative shopping opportunities at times when we consider them most relevant. [...]
>
> 5. Display of Advertising. The Software will collect information about you and the websites you visit ("Usage Data"), but will not collect information that will be used to identify you personally. This information will be used to provide you with comparative shopping opportunities when they are most relevant. By installing and/or using the Software you grant permission for 180solutions to periodically display sponsors' websites to you, and to collect, use and disclose the Usage Data The frequency of the advertisements will vary depending on your use of the Internet. You acknowledge that the Software includes an anonymous user ID and an electronic cookie that enables 180solutions to collect such information and to display advertising targeted to you. A "cookie" is a small amount of data that 180solutions' servers transfer to your browser and that only 180solutions' servers can read. You understand that 180solutions does not control your interaction with the websites and advertisements displayed to you and we assume no responsibility for their content or privacy practices and policies.

The Zango EULA contains similar language and clauses.

The advertising is delivered in the form of browser windows opened on the user's desktop. The major problem with these advertising windows is that they take the form of standard Internet Explorer windows that are well nigh indistinguishable from pop-ups and windows opened by the web sites that users are directly visiting. Although the title bar for these special advertising windows carries the text "Brought to you by the 180search Assistant" or "Brought to you by the Zango Search Assistant," many users will not notice that title bar text or recognize it as being connected with software locally installed on their computers. Moreover, these ad windows carry no information about how to stop the display of such unwanted advertising.

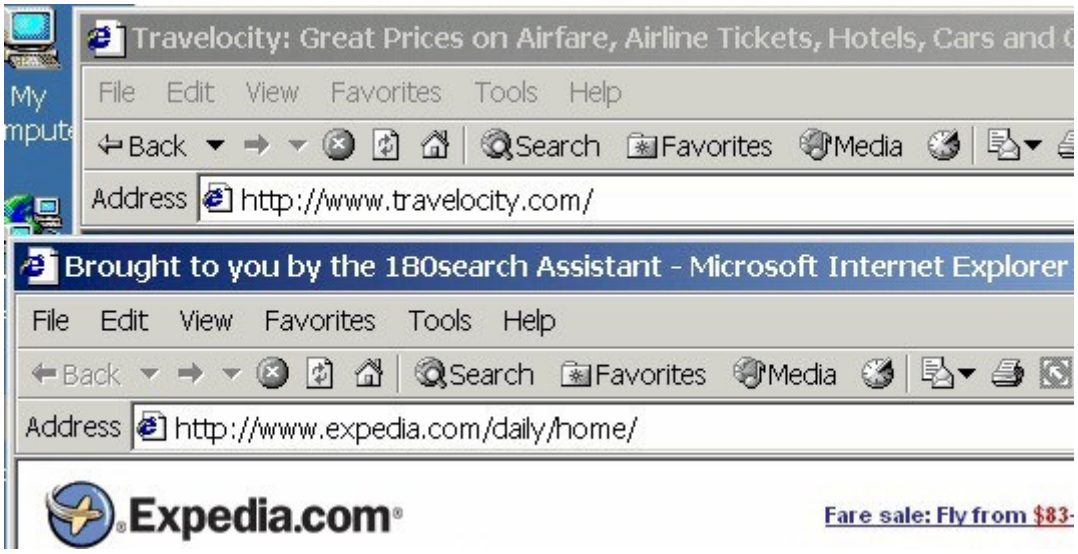

Figure 5: 180search Assistant advertising

Even that default title bar text may disappear and be replaced by other text should the opened web page automatically redirect to another web page, making it still more difficult for users to distinguish 180's advertising from the advertising users encounter at web sites they have deliberately visited.

Still more disturbingly, 180solutions resorts to descriptions, claims, and euphemisms on its web site and in the text displayed to users during installation of newer versions of its software that, at their best, are less than helpful and, at their worst, are arguably deceptive. For example, instead of using straightforward unvarnished language to clearly warn users that the software will open advertising pop-ups on the desktop, the installer screen for the new version of the 180search Assistant resorts to such language as "comparison web sites" to describe the software's pop-up advertising. On its "Privacy Pledge" web page (http://www.180solutions.com/pages/privacypledge.aspx), 180 employs similarly sterilized language:

> 180search Assistant, a 180solutions permission-based search assistant application, provides free access to screensavers, toolbars and downloads in exchange for showing you an average of two to three targeted websites daily when you search or shop online.

On the same page 180 employs confusing, slippery constructions that are arguably designed to induce the mistaken impression among readers that its software doesn't display advertising:

> We do not display non-permission-based advertising such as banner ads or pop-ups. All of the sponsor websites served by 180solutions are easily closable browser windows clearly identified as 'Brought to you by the Zango Search Assistant' or 'Brought to you by the 180search Assistant.'

180 goes even further on its FAQ page, presenting a series of questions and answers, the sum total effect of which can be described only as deliberately and calculatingly false and deceptive (http://www.180searchassistant.com/faq.html):

> Can I have ad delivery software installed while I have 180search Assistant?
>
> Yes, 180search Assistant is a search assistant that helps you find the product information and offers that match what you are looking for online. 180search Assistant does not interfere or prohibit your ability to install other ad delivery software that might be required by some free software applications.
>
> Does 180search Assistant show pop-up ads?
>
> No. 180search Assistant does not show pop-up ads - it only shows you websites we match up to targeted keywords that you type into shopping sites or search engines. Uninstalling 180search Assistant will NOT prevent you from getting pop-up ads.
>
> So 180search Assistant only shows me other websites?
>
> Yes, 180search Assistant is designed to scour a huge database of product information and offers to help you find what you are looking for when searching or shopping online. 180search Assistant is not designed to interrupt your online entertainment with annoying intrusions.
>
> How often does 180search Assistant show me websites?
>
> A typical 180search Assistant user is shown 2-3 websites over a 24-hour period. The number of sites 180search Assistant shows can depend on how actively you search or shop online, but is designed to highlight the right information or offer at the right time instead of bombarding you with useless information.
>
> Where do pop-up ads come from?
>
> Many websites include pop-up ads with the other advertisements they show to support their sites. In addition, other advertising applications can also show you pop-up ads. However, 180search Assistant does not control those pop-up ads.

180 clearly strives to give readers the false impression that it does not display unwanted advertising on the user's desktop and that any such advertising must surely be caused by other, unrelated software.

Data Collection, Transmission, & Sharing

180solutions goes out of its way to insist on the privacy-friendly nature of its advertising software. Its web sites display a set of rotating, animated logos:

Figure 6: 180solutions' "Privacy Pledge" animated logos

180solutions' software does monitor users' web surfing, collect data about that web surfing, and use that data to display advertising. Moreover, that web surfing data is transmitted to 180solutions and tied to a unique ID number to distinguish unique installations. 180 claims that it does not surreptitiously collect Personally Identifiable Information, however. From the 180search Assistant EULA (http://www.180searchassistant.com/eula.html):

> 180search Assistant will periodically direct you to our sponsors' websites. 180search Assistant will collect information about the websites you visit, but will not collect any information that will be used by 180solutions to identify you personally. The information that 180search Assistant collects and transmits to 180solutions will be used to provide you with access to comparative shopping opportunities at times when we consider them most relevant. [...]
>
> 5. Display of Advertising. The Software will collect information about you and the websites you visit ("Usage Data"), but will not collect information that will be used to identify you personally. This information will be used to provide you with comparative shopping opportunities when they are most relevant. By installing and/or using the Software you grant permission for 180solutions to periodically display sponsors' websites to you, and to collect, use and disclose the Usage Data The frequency of the advertisements will vary depending on your use of the Internet. You acknowledge that the Software includes an anonymous user ID and an electronic cookie that enables 180solutions to collect such information and to display advertising targeted to you. A "cookie" is a small amount of data that 180solutions' servers transfer to your browser and that only 180solutions' servers can read. You understand that 180solutions does not control your interaction with the websites and advertisements displayed to you and we assume no responsibility for their content or privacy practices and policies. [...]
>
> 8. Collection of Information. 180solutions collects and uses certain information about you from your use of the Software. By installing the Software, you grant permission for 180solutions to collect this information, including the websites you visit while connected to the Internet."

This data collection and transmission is described further in 180's Privacy Policy (http://www.180searchassistant.com/privacy.html):

> By installing 180search Assistant, you grant permission for 180solutions to periodically display targeted websites, to collect certain information, including the websites you visit while connected to the Internet, and to use that information as described herein. 180solutions will not use any of the information 180search Assistant collects to identify you personally.
>
> 180search Assistant. The 180search Assistant software ("180search Assistant") is a permission based search assistant application that provides access to a wide range of websites, applications and information. 180search Assistant will periodically direct you to our sponsors' websites. The information that 180solutions collects under this privacy policy allows 180search Assistant to provide you with content and advertising that is targeted to your interests.
>
> What We Collect. When the 180search Assistant software is actively running on your computer, it generates logs of your web browsing activity, including web pages you have visited and the order in which you visited these pages. These logs are then uploaded to 180solutions' servers, along with an anonymous user ID assigned to the 180search Assistant software installed on your computer (your "Anonymous User ID"). We use these logs for market research purposes and to allow 180search Assistant to provide you with content specifically targeted to your interests at the time when the content is relevant. 180solutions stores these logs on our servers, for our use. We may aggregate information from these logs and share the aggregate data with third parties. The 180search Assistant software will also put a "cookie" on your machine so that we are able to recognize you and display

> appropriate targeted websites. A Cookie is a small amount of data that 180solutions' servers transfer to your browser and that only 180solutions' servers can read.
>
> Treatment of Personal Information. While complete URLs are collected by the 180search Assistant software and uploaded to our servers, efforts are taken to strip away any information that could be used to identify you personally before URLs are stored. While we cannot guarantee that all such information will be stripped away by our systems, 180solutions will not use any of the information 180search Assistant collects to identify you personally.
>
> Opt In Information. Occasionally, 180solutions may display additional questions to you, inviting you to opt in and supply information that may include demographic information. This demographic information may include, but is not limited to, your age, gender, geographic region and interests. This demographic information is linked to your Anonymous User ID, and is not connected or linked to information that will be used to identify you personally. Any answers you supply are covered by this privacy policy. 180solutions uses this information to learn more about its audience and may share this information with third parties. 180solutions also uses this demographic information to provide you with content and information most likely to be relevant to you.

In his write-up on 180's software, Andrew Clover claims that "some nc variants also seem to try to read an e-mail address, real name and ZIP code to associate with the unique identifier, from applications' data in the registry" (http://www.doxdesk.com/parasite/nCase.html). Sunbelt has not observed such behavior in its own testing, and this functionality may be confined to older versions of 180solutions' software.

The new versions of the 180search Assistant and Zango incorporate a tray icon that allows users to disable "logging." The logging being referred to is the applications' "tech support logging," which is a record of key software performance events, including URLs captured from the user's surfing activity. This log data are stored in the files Sau.log or Zango.log (found in the applications' respective installation directories). These logs are uploaded periodically to 180's servers and tied to an anonymous "User ID" (as noted in the previously quoted EULA and Privacy Policy).

When the user disables "Logging," all logging to that file ceases, though the file itself and previous data contained there-in remain. Moreover, because this ability to disable "Logging" is nowhere documented or explained to the user (the feature exists without comment or explanation in the tray icon menu), many if not most users will not recognize it for what it is and take advantage of it, substantially reducing the usefulness of this feature.

Uninstallers

All versions of 180solutions' software have offered uninstallers of some sort, though the uninstallers included in the newer versions of the 180search Assistant and Zango differ in some ways from the uninstallers included in older versions of 180's software. 180solutions emphasizes on its web site that its applications are easily removed: "Our programs can be easily removed at any time by going to the “Add/Remove Programs” menu on your computer and clicking the “remove” button next to the entries for our applications" (http://www.180solutions.com/pages/privacypledge.aspx). While the uninstallers included in the newer versions of the 180search Assistant and Zango are somewhat changed, there is still substantial room for improvement.

Old versions

With older versions of 180's software, users who attempted to remove the software through the Add/Remove Programs Control Panel applet were informed that they had to have an internet connection, because the uninstaller connected to 180's web site and downloaded and executed yet another uninstaller. Without an internet connection, the uninstallation process failed. Some versions of 180's software required the user to run not one but two uninstallers, each of which needed access to the internet. In cases where the PCs internet connection had been broken (perhaps by other programs installed along with 180's software that modified the Winsock LSP stack/chain), users were forced to remove the software manually or resort to an anti-spyware application.

New versions

The newer versions of 180's software include uninstallers that can remove the software without a connection to the internet. This uninstaller does briefly pester the user to keep the software, but ultimately the uninstaller does work, performing a reasonably clean removal of the installed files and Registry keys.

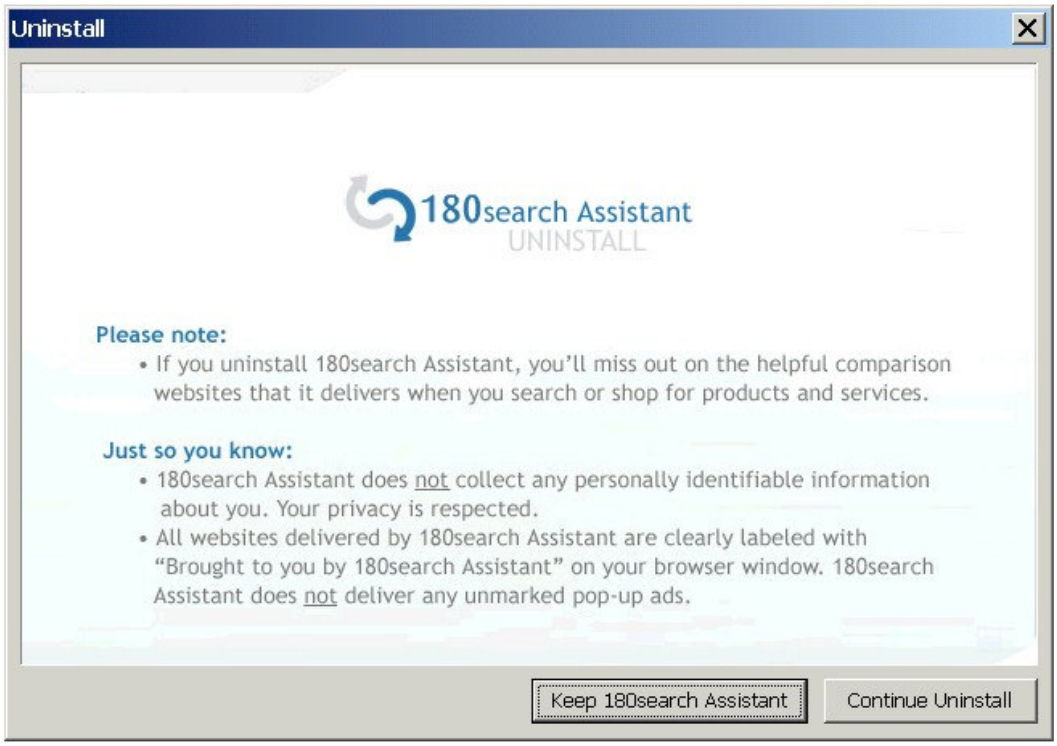

Figure 7: 180search Assistant "Uninstall" screen

It should be noted that both Andrew Clover and Ben Edelman have complained of incomplete removals, though they may have been referring primarily to older versions of 180's software -- see http://www.benedelman.org/spyware/180-affiliates/installation.html and http://www.doxdesk.com/parasite/nCase.html.

Where 180's software is installed to support the use of a "freeware" application (either from a third-party or from Zango), 180's programs will not automatically uninstall or prompt the user to uninstall when the host "freeware" application itself is removed.

Still further, in one case encountered during Sunbelt's testing, the 180 uninstaller falsely warned that 180's software was required to support a "freeware" application that was not even present on the test computer.

Figure 8: 180search Assistant "Uninstall" warning

Of more concern, though, is the "resuscitator" program that is silently installed by the new 180search Assistant to the Windows directory.

This program is a randomly named, UPX-packed executable that is configured to start with Windows through the HKEY_LOCAL_MACHINE\...\Run key. File size is 46,080 bytes. Given its characteristics, this program is clearly designed to avoid detection by anti-spyware applications.

Moreover, the sole purpose of this program is to monitor the installed 180 files and prompt the user to reinstall the application should those files be removed.

Figure 9: 180search Assistant "Resuscitator" prompt

Tray Icon

As noted earlier, the new versions of the 180search Assistant and Zango display tray icons next to the clock on the Windows taskbar while running. Older versions of 180's software gave very little evidence to users that they had been installed, with no tray icon or other visible indication of the software's presence on the computer (aside from the advertising opened on users' desktops). The new versions of the 180search Assistant and Zango do display tray icons, however, from which users can access limited information about the software.

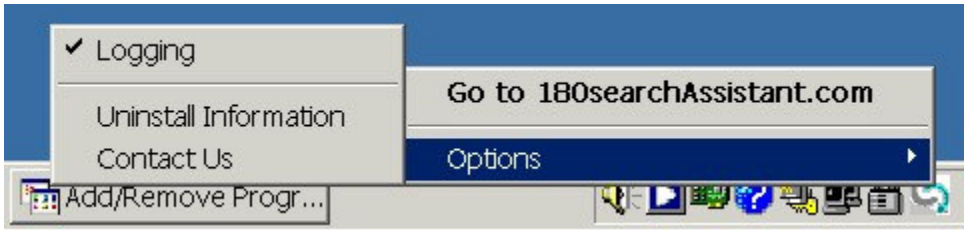

Figure 10: 180search Assistant tray icon

While this tray icon does represent a minor improvement to the software's functionality, many users might not notice the tray icon amidst the typical clutter of other icons next to the clock. Still further, because 180's advertising can be difficult to distinguish from normal internet advertising that users encounter at web sites, many users might not make the connection between the tray icon and the additional advertising windows that appear on their desktops.

"CBC Force Prompt"

The most significant change to newer versions of the 180search Assistant and Zango is the use of a "CBC Force prompt" to automatically notify users of the installation of 180solutions' software when these new program versions are installed and executed for the first time. Indeed, on its web site 180solutions trumpets the claim that its "programs are only downloaded with user consent and opt-in" (http://www.180solutions.com/pages/privacypledge.aspx).

Just how this "CBC Force prompt" is displayed to users and the text used in that display differs, depending on the context of installation.

New versions downloaded directly from 180's own web sites

The newer versions of the 180search Assistant and Zango available directly from 180solutions' own web sites employ a "CBC Force prompt" that displays the following text during installation:

```
You are about to install 180search Assistant, a small desktop
application that delivers you comparison websites when you search or
shop online. You are shown on average two or three websites daily.
180search Assistant:

* Does not collect any personally identifiable information
about you. This program collects information about web
pages you browse to display relevant advertisers' web sites.
```

```
* When running, this program is represented by an icon in
your system tray. The Search Assistant can be easily
uninstalled at any time by clicking the icon or going to
"Add/Remove Programs" in your control panel an
selecting 180search Assistant.

By selecting "OK" you agree to the terms and conditions of the user
license agreement. (http://www.180searchassistant.com/eula.html)
```

As noted earlier, the language used in this notice screen relies too heavily on sterilized euphemisms that do little to alert users to potentially objectionable behavior, especially when those users are presented such unremarkable text in the midst of a bundled installation. Combined with the disturbingly misleading claims on 180's web sites (documented above), this "CBC Force prompt" is but a very minor improvement in the notice and disclosure practices employed during the installation of 180's software.

Updates to older third-party installations

The "CBC Force prompt" text that should be displayed to users differs when older versions and installations of the 180search Assistant are auto-updated to the newer "CBC Force prompt" enabled version. More importantly, however, Sunbelt has uncovered disturbing evidence that this "CBC Force prompt" is being bypassed when older versions and installations of the 180search Assistant are updated to the latest, COAST-certified version.

As previously discussed, 180solutions uses a variety of distribution channels to deliver its software to users' desktops, including third-party "partners" who may bundle the 180search Assistant with their own applications or install it from their own web sites. One notable problem with these third-party distributors has been the widespread use of poorly disclosed installations of 180's software (*e.g.*, EULA-only installations, or worse) and "force-installs," many of them done via security exploits or Windows Media Player files. Given this checkered installation history, two concerns loom large for the anti-spyware community:

1. *The status of older installations* -- what will 180solutions do with older installations of its software, many if not most of which amount to "ill-gotten gains" from illegal "force-installs"?

2. *The status of older installers used by rogue distributors* -- what will 180solutions do about distributors who possess copies of installers that drop old versions of 180's software on user's desktops and who continue using these older installers?

Clearly this "CBC Force prompt" is intended to thwart rogue distributors who might seek to install 180's software without proper notice and disclosure. Indeed, 180solutions claims on its web site that it vigorously monitors third-party distributors (http://www.180solutions.com/pages/privacypledge.aspx):

> All 180solutions' third-party distributors are required to clearly label that our programs are bundled with their products and to provide consumers with the option to agree to the licensing agreement before they install it. We police distributors to ensure our disclosure rules are adhered to and we

> prohibit “drive-by” or “silent” installations. Our code of conduct requires that the user is fully aware of and agrees to our End User License Agreement (EULA).

There are good reasons to be skeptical of such claims. For one, as Mr. Sawicki himself has been forced to acknowledge, these rogue affiliates has proven to be nothing if not resourceful in concocting methods and means to rip apart software bundles and install 180's software without proper notice and disclosure, and the pay-per-install affiliate networks employed by 180solutions give them every incentive to do so.

Moreover, 180's expressed desire to dissociate itself from or minimize its responsibility for the behavior of its rogue affiliate distributors does not inspire confidence in 180's willingness or ability to rein in distributors who might somehow devise methods to thwart or undermine what little additional notice is offered by these new installers. Still further, there is no guarantee that 180 can't and won't at some future point in time develop more "affiliate friendly" installers that would dispense with this new "CBC Force prompt."

But there is an even more serious reason to doubt 180's commitment to breaking with its checkered past of deriving economic benefit from illegal "force-installs." As noted above, the new versions of the 180search Assistant and Zango use a "CBC Force prompt" that is "hard coded into the client," according to representations made by 180solutions to Sunbelt. Although 180 has claimed that this "CBC Force prompt" "cannot be turned off" and should be displayed during "all installs" of 180's software, this simply isn't the case, and Sunbelt has documented examples of installations of newer versions of the 180search Assistant where the "CBC Force prompt" was in fact not displayed to the user.

"CBC Force Prompt" Registry Flag

To understand why the "CBC Force prompt" might not be displayed to users during installation, it is necessary to explain how 180's client software determines whether to show the "CBC Force prompt." The newer versions of 180search Assistant and Zango set a "flag" in the Registry, and this flag indicates whether or not the user has seen the "CBC Force prompt." The flag consists of the following Registry value, where "client" is the variable name of main executable, and "X" can be a value of "0" or "1":

```
[HKEY_CURRENT_USER\Software\client]
"cbc"=dword:0000000X
```

The key data is the dword value. A dword value of "0" means that the user has not seen the "CBC Force prompt" and that the prompt should be displayed. A dword value of "1" means the user has already seen the "CBC Force prompt," which should not be displayed again.

If the dword value is set to "0," the 180search Assistant pops up either the "CBC Force prompt" text quoted earlier or, in cases where the software has updated an older version of the 180search Assistant, a box with the following text:

```
180search Assistant is a component program you recently
installed.
```

```
This program is represented by an icon in your system tray and
can be easily uninstalled from Add/Remove Programs in your
Control Panel. You will receive an average of 2-3 advertiser
referrals daily, based solely on keywords from web sites you
visit to help you find exactly what you are looking for, faster.

By selecting "OK," you agree to the Terms and Conditions of the
user license agreement.
```

This text, it should be noted, consists of the same sterilized euphemisms used in the main "CBC Force prompt" displayed during completely new installations of the most recent versions of 180search Assistant and Zango downloaded directly from 180's own web sites. If the user selects "OK," the software is retained on the PC. If the user cancels out of the prompt box, the 180search Assistant confirms whether the user wants to uninstall. If the answer is "yes," the 180search Assistant uninstalls itself.

These events are recorded in the log file maintained in the 180search Assistant or Zango directory. For example, the following lines log an installation in which the "CBC Force prompt" was displayed to the user during a new installation of the latest version of the 180search Assistant downloaded directly from 180searchassistant.com:

```
03/04/05 04:17:51 1096 1124 0 2 1009 0 CBC initialize request detected -
   performing CBC check CCBC.cpp 36 sau 6.6 004217
03/04/05 04:17:51 1096 1124 0 2 1178 0 Forcing CBC dialog CCBC.cpp 73 sau
   6.6 004217
03/04/05 04:19:01 1096 1124 0 2 1087 0 user accepts cbc CCBC.cpp 52 sau
   6.6 004217
```

If the dword value is set to "1," however, the "CBC Force prompt" is not displayed at all. This turn of events is also logged:

```
03/08/05 18:12:58 1312 1348 0 2 1009 0 CBC initialize request detected -
   performing CBC check CCBC.cpp 36 sais 6.6 841 247toynenemjrpsuususlwsr
   fnllch 841 368024987
03/08/05 18:12:58 1312 1348 0 2 1085 0 user has already seen cbc dialog
   CCBC.cpp 58 sais 6.6 841 247toynenemjrpsuususlwsrfnllch 841 368024987
```

Problems with the Registry Flag

This mechanism for determining whether or not to display the "CBC Force prompt" is entirely inadequate to the job of ensuring that rogue distributors do not "force-install" the 180search Assistant on users' PCs without those users receiving notice of the installation of 180's software.

At the very least, the "CBC Force prompt" Registry flag is trivially easy to hack, and it is not too difficult to imagine rogue distributors building installers that set this Registry flag to indicate to 180's software that users have already seen the "CBC Force prompt" when in fact they have not.

Sunbelt has not discovered any installations in which such a hack appears to have been perpetrated, but given the economic incentives for distributors to install 180's software (which is largely unwanted by users) as well as the ease of performing the hack, it seems likely to happen.

180solutions Itself Bypasses the "CBC Force prompt"

More disturbingly, however, it appears that 180solutions is itself electing to bypass the "CBC Force prompt" in order to avoid alerting users to the installation of 180's software, and the implications of this are serious.

As discussed earlier, Sunbelt observed several installations of older versions of the 180search Assistant in which that software was updated to the latest version. After older versions of the 180search Assistant were "stealth-installed" via a Windows Media Player file and via a Java applet at lyricsdomain.com, that software called out to 180's servers, and downloaded and installed the latest, COAST-certified version of the 180search Assistant.

Given that these older versions had been "force-installed" and had not displayed any sort of notice and disclosure to the user, the "CBC Force prompt" should have been displayed to the user once the latest version of the 180search Assistant had been installed and executed for the first time. In fact, the "CBC Force prompt" was never displayed; the new version simply installed silently, added its tray icon to the Windows taskbar, and began its normal routine of updating the "trigger" .DAT files and serving up advertising.

After re-testing, Sunbelt discovered that this new version of the 180search Assistant was adding the `"cbc"=dword:0000000X` value (which is unique to the latest versions of the 180search Assistant and Zango) to the Registry, but setting it to "1," thus indicating that the user had already seen the "CBC Force prompt" when in fact the user had seen no such prompt. (Figure 11 shows the "CBC Force prompt" that should have been displayed but was in fact not displayed.)

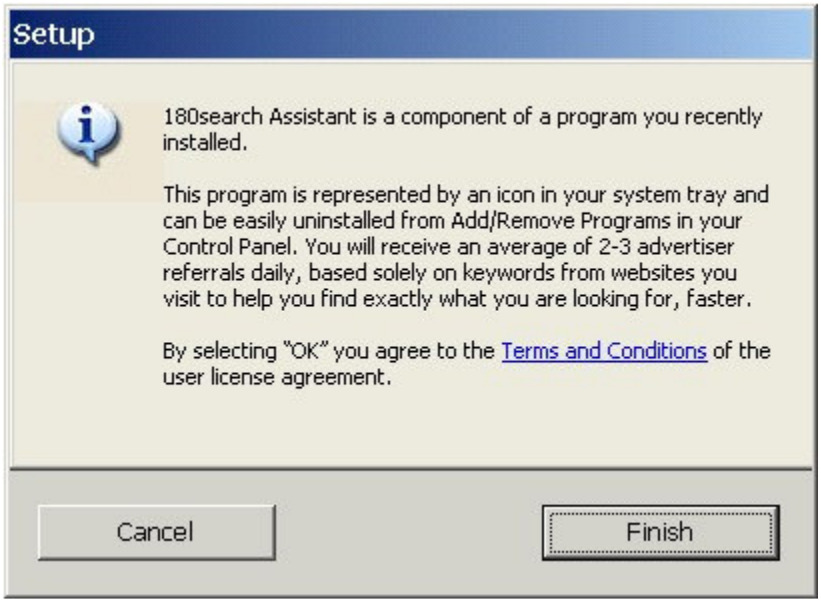

Figure 11: 180search Assistant "CBC Force prompt" (update)

Sunbelt knows of at least one other installation of an older version of the 180search Assistant maintained by a reputable security researcher. This researcher reports that the installation has

been maintained since July 2004, meaning that the software originally installed was an older, pre-COAST-certified version of the 180search Assistant. This researcher reports recently inspecting the Windows Registry and discovering that the `"cbc"=dword:0000000X` value had been added to the Registry and set to "1." Moreover, this researcher discovered that the software itself had been silently updated to the latest version of the 180search Assistant. At no time did this researcher ever see a "CBC Force prompt" -- the software was merely updated, the "CBC Force prompt" bypassed, and the Registry flag set to indicate falsely that the user had seen the "CBC Force prompt."

Implications of 180's False Setting of the "CBC Force Prompt" Registry Flag

The implications of 180solutions' apparent decision to silently update old installations of its software and set the "CBC Force prompt" Registry flag to indicate falsely that the user has seen the prompt are several and serious.

1. 180solutions has elected to maintain older installations of the 180search Assistant

By silently updating older installations of the 180search Assistant performed prior to January 2005 to the latest software version without displaying the "CBC Force prompt," 180solutions has effectively elected to continue to maintain, service, and derive economic benefit from those older installations, many if not most of which 180solutions must surely know are the products of illegal "force-installs" in which victims received no notice whatsoever that 180's would be installed and in which their consent to those installations was never gained.

2. 180solutions has elected to maintain newer "force-installations" of the 180search Assistant

As noted earlier, many rogue distributors possess installers that drop older versions of the 180search Assistant on users' PCs. As Sunbelt discovered, these older installers are still being used to "force-install" 180's software on users' PCs. In some cases these older versions may be silently updated to the latest version of the 180search Assistant and the "CBC Force prompt" never displayed. By silently updating these new installations of older software versions, 180solutions has effectively elected to maintain, service, and derive economic benefit from new "force-installs" of its software.

It is important to reiterate that 180solutions itself claims that third-party distributors are required to provide notice and disclosure during installation of its software. As quoted earlier (http://www.180solutions.com/pages/privacypledge.aspx):

> All 180solutions' third-party distributors are required to clearly label that our programs are bundled with their products and to provide consumers with the option to agree to the licensing agreement before they install it. We police distributors to ensure our disclosure rules are adhered to and we prohibit "drive-by" or "silent" installations. Our code of conduct requires that the user is fully aware of and agrees to our End User License Agreement (EULA).

As Sunbelt discovered, this claim is substantially false, incomplete, and misleading, given what is in fact occurring when installations of older versions of the 180search Assistant are updated to the latest version.

Putting "Bad Apples" in with "Good Apples"

It should also be noted that 180solutions could have implemented and rolled out its new software differently so as to make a clean break with its checkered past of "force-installs" and installs done with poor notice and disclosure. What it could have and should have done was set up a new server on a new sub-domain of 180solutions.com unknown to older versions of its software. It could have then hard coded its new software versions to update only from that new server, leaving older software versions to update from the old servers. It could have then pushed an uninstaller down onto those older installations to remove them from users' systems.

The net effect of this scheme would be to break the older installations of 180's software and ensure that the latest versions were installed and maintained separately via 180's servers. This scheme would also effectively break the newer stealth installations being performed by rogue distributors with old installers.

But 180solutions did none of this. Instead of breaking its older installations, many if not most of which are the product of illegal "force-installs," 180solutions has elected to maintain those older installations by allowing those older software versions to update to the latest version. And instead of breaking those older installers, many of which are still being used to "stealth-install" 180's software on victims' PCs, 180solutions has elected to enable those installers to continue to be used by allowing the old software versions dropped on users' PCs by those installers to update to the latest version of the 180search Assistant. And, of course, 180 has apparently elected to update those older installations and versions without displaying the "CBC Force prompt," entirely contrary to its representations to Sunbelt.

In taking these actions, 180solutions has made it next to impossible for "anti-spyware" programs like Sunbelt CounterSpy to distinguish between older installations, which may have been the "illegitimate" product of "force-installs," and newer installations which might presumably be less likely to have been the product of "force-installs." Because older versions of the 180search Assistant can update to the latest version, and because Sunbelt has no way to determine the context of installation merely by scanning a user's hard drive (not to mention that the "CBC Force prompt" Registry flag might have been falsely set by 180solutions itself), Sunbelt effectively has no way to sort out "legitimate" installations of 180's software from "illegitimate" ones. 180solutions has essentially put the "bad apples" in with the "good apples" (and has arguably attempted to make "bad apples" look like "good apples"), thus forcing Sunbelt to assume that any installation of 180's software that it encounters might be potentially "illegitimate" and a fair target for detection and removal.

Summary

It can be anticipated that 180solutions will argue that even if the "CBC Force prompt" Registry flag is incorrectly set during updates of older versions of its software to the latest version, the new tray icon effectively serves as notice to users of the software's presence and that users still derive benefit from the new, revamped uninstaller. This argument should be firmly rejected because most users are not likely to notice this new tray icon amidst the typical clutter of other

icons next to the clock on the Windows taskbar. As a form of notice and disclosure, the tray icon is entirely inadequate. Moreover, in the case of "force-installs," 180's software should never have been on the PC in the first place, tray icon or not. These are illegal "force-installs" and 180solutions should be making no effort whatsoever to maintain, service, and derive economic benefit from them.

In sum, contrary to all the claims 180solutions has made for this new "CBC Force prompt," Sunbelt cannot regard it as sufficient grounds for treating newer, COAST-certified versions of 180's software any differently from older versions.

Conclusion

Both COAST and 180solutions have claimed that the new versions of the 180search Assistant and Zango incorporate changes that amount to substantial improvements in the software's functionality, making 180's advertising programs vastly more privacy-friendly and transparent to users. Moreover, 180solutions continues to maintain that it is cleaning up its distribution channels to put an end to the problem of rampant "force-installs" of its software by rogue third-party distributors. 180 insists that it is vigorously policing its distribution "partners" and claims that the new "CBC Force prompt" incorporated into the new versions of the 180search Assistant and Zango should ensure that users always receive proper notice and disclosure of the software's installation.

Having looked into these new COAST-certified versions of 180solutions' advertising applications, Sunbelt Software cannot agree with any of these claims. Not only does Sunbelt regard the changes to 180's advertising, uninstallation, and data collection practices to be at best only minor improvements, but Sunbelt has documented an extremely disturbing pattern of behavior by 180solutions itself, which appears to be silently updating older installations of its software while deliberately bypassing the "CBC Force prompt" that should be displayed to notify users to the presence of 180's software.

In electing to silently update these older installations and software versions, 180solutions has apparently decided to continue to service, maintain, and derive economic benefit from installations of its software that 180 surely knows are the likely products of illegal "force installs. Such behavior in no way comports with the representations made to COAST or the wider anti-spyware community concerning 180solutions' efforts to clean up and police its software distribution channels. Far from reining those rogue third-party distributors in, 180solutions appears to be taking active steps to continue profiting from unethical installations performed by those rogue distributors.

Sunbelt Software
March 13, 2005

References

180search Assistant EULA
http://www.180searchassistant.com/eula.html

180search Assistant FAQ
http://www.180searchassistant.com/faq.html

180solutions "Privacy Pledge"
http://www.180solutions.com/pages/privacypledge.aspx

180solutions Privacy Policy
http://www.180searchassistant.com/privacy.html

Adware Installed through WMA Files
http://www.dslreports.com/forum/remark,12245912~mode=flat

Andrew Clover: nCase
http://www.doxdesk.com/parasite/nCase.html

Ben Edelman: 180solutions Installation Methods and License Agreement
http://www.benedelman.org/spyware/180-affiliates/installation.html

Ben Edelman: 180 Talks a Big Talk, but Doesn't Deliver
http://www.benedelman.org/news/011705-1.html

Ben Edelman: Media Files that Spread Spyware
http://www.benedelman.org/news/010205-1.html

Ben Edelman: Who Profits from Security Holes?
http://www.benedelman.org/news/111804-1.html

Breaking, Entering Your PC (L.A. Times, 26. Nov. 2004)
http://www.latimes.com/news/nationworld/nation/la-na-spyware26nov26,0,7513997.story?coll=la-home-headlines

CDT: Testimony of Ari Schwartz before the House Committee on Energy and Commerce on 26 Jan. 2005
http://www.cdt.org/testimony/20050126schwartz.pdf

Eric L. Howes - The Anatomy of a Drive-by-Download
https://netfiles.uiuc.edu/ehowes/www/dbd-anatomy.htm

Internet advertiser disputes 'adware' label (Seattle Post-Intelligencer, 2 Apr. 2004)
http://seattlepi.nwsource.com/business/167416_180folo02.html

News: Major Exploit Underway...
http://www.dslreports.com/forum/remark,11904374~mode=flat

Risk Your PC's Health for a Song?
http://www.pcworld.com/news/article/0,aid,119016,00.asp

WMP Adware: A Case Study in Deception
http://www.dslreports.com/forum/remark,12298989~mode=flat~start=0

About Sunbelt Software

Headquartered in Tampa Bay (Clearwater), Fla., Sunbelt Software was founded in 1994 and offers products to protect and secure systems from costly inefficiencies including spam and spyware; as well as enterprise solutions to protect against system downtime and security vulnerabilities.

Sunbelt Software is part of the Sunbelt International Group, which includes Sunbelt Software, Inc. and Sunbelt System Software in Europe. The Sunbelt System Software group has offices in the UK, France, Netherlands, Sweden and Germany.