iDEFENSE
A VeriSign Company

VeriSign

// THE POWER OF INTELLIGENCE

Top-10 Spyware Threats

An iDefense Security Report
iDefense Intelligence Operations

Jan. 6, 2006

Table of Contents

1 Introduction

As most people herald the arrival of 2006 with fanfare, the creators of spyware and adware applications continue inexorably toward the goal of maximizing revenue from their creations. The automatons that they set into motion do not take holiday breaks, preferring instead to lie in wait for the next user gullible enough to download, install and use the malicious software and provide financial benefit to the spyware distributors. Spyware is a perfect example of the growing trend in which questionable entities exploit the Internet for financial gain. The last few years have proven that malicious code, and its cousins adware and spyware, have become the *raison d'être* for many computer professionals. Additionally, the fine line between the malicious code camp (writing and distributing worms, viruses, Trojan horses and combinations thereof) and that of adware and spyware (writing code that is "questionable" at the least) is blurring, and successful techniques used by one faction are often, and quickly, incorporated into the products of the other. There is even a fast-growing trend of adware and spyware being deployed by means of malicious code droppers and websites - all in the pursuit of easy money.

What, exactly, are adware and spyware? The answer depends on the source, and 10 people (or 10 online definitions) would return 10 distinct answers. However, at the core of all responses would be the words "unwanted," "questionable" and "unknowingly." For this reason, with regard to this report, iDefense refers to both adware and spyware applications as "spyware." Furthermore, iDefense defines "spyware" as:

> *Unwanted or questionable code that is installed on a computer without the users' explicit knowledge and which is designed to monitor and report upon, in any manner, activity of the users or the computer upon which it is installed.*

This definition is, of course, different from those already found online, but does summarize the essence of spyware. It is important to note that nowhere in the iDefense definition is the term "illegal" used. This is because spyware applications are legal under today's regulatory legislation. Note also that the definition is conservative and non-judgmental in its terminology, lessening the civil liability associated with publishing an article of this nature.

Irrespective of legality, however, spyware is a substantial drain on all computer users' financial resources.

2 Spyware Financial Impact

In 2004, the spyware industry is estimated to have earned more than $2 billion through the distribution and installation of applications designed to monitor and report its victim's activities (Webroot Software Inc., State of Spyware Q1-2005, April 2005).

Conversely, the corporate anti-spyware industry earned an estimated $100 million and is projected to reach $1.2 billion in revenue by 2010 (The Radicati Group, http://www.radicati.com/cgi-local/brochure.pl?pub_id=511&subscr=&back_link=/reports/single.shtml, June 2005).

A recent America Online/National Cyber Security Alliance study showed that 61 percent of personal computers contained spyware that the user did not know about (AOL/NCSA Online Safety Study, http://www.staysafeonline.info/pdf/safety_study_2005.pdf). Furthermore, an evaluation of the "best" anti-spyware packages showed that no single package can remove all spyware, which means that more than one anti-spyware package must be purchased and used to ensure that a computer is secure. And, as if preventing and removing spyware were not expensive enough, regulations such as the Sarbanes-Oxley Act of 2002 - Section 404 (SOX 404), the Gramm-Leach-Bliley Act of 1999 (GLBA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) place the onus of securing data on the shoulders of the business entities housing said data, without consideration for potential intrusions caused by legitimate or non-legitimate spyware applications. Consequently, a breach of these regulations may result in additional financial loss.

3 Brief History of Spyware

3.1 Cookies

Like most technological advances, spyware began as a well-intentioned concept - to improve the "user's Internet experience." As Internet popularity increased, and websites supported more user interaction, it became desirable for the website and user to share historical information about the user's surfing habits. To accomplish this, a means was needed to allow the Web server to send the browser information about visits to the website. This communication took place in the form of a "cookie," a term derived from the whimsical "magic cookie" tokens employed by UNIX to track users or programs.

There are two types of cookies used for tracking website visits, the transient (aka, "session") cookie and the persistent (aka, "permanent") cookie. A transient cookie is designed to track a single visit, while a persistent cookie is intended to aid the user over the course of multiple visits. Transient cookies are resident in memory and deleted when the browser is closed. Persistent cookies, on the other hand, are saved as text files in the computer's permanent storage.

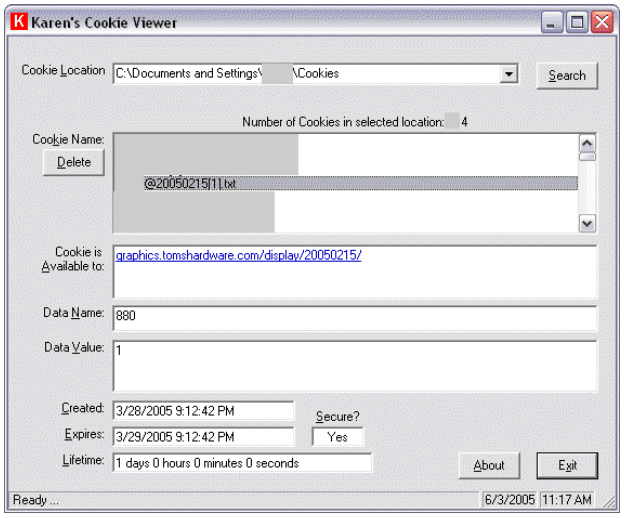
As initially designed, all cookies were intended for use only by the website issuing the cookie, and allowed users to configure cookie options to receive a more "customized" experience from the website. A cookie allows a Web browser and Web server to communicate using the following six parameters:

- Cookie Name
- Availability (Domain and/or page)
- Data Name
- Data Value
- Date expires
- Security settings

An example of the code of a typical cookie follows:

```
880
1
graphics.tomshardware.com/display/20050215/
1600
190791936
29701284
3776685728
29701082
*
```

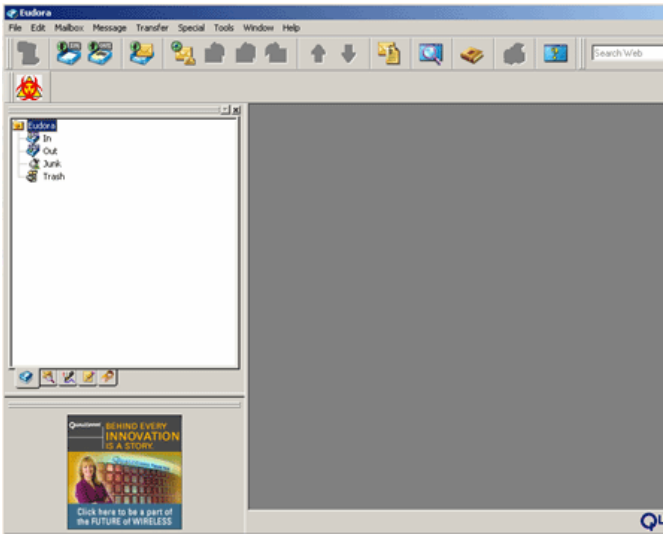
Or, as displayed in "Karen's Cookie Viewer" (http://www.karenware.com/powertools/powertools .asp):



Karen's Cookie Viewer Tool

3.2 Adware Applications

Adware began, and continues today in some form, as a means to support programmers wishing to freely distribute their applications while still receiving compensation. A good example of an earlier adware application is WeatherBug. Users could download and install WeatherBug for free, provided they selected "sponsors" from whom they would receive e-mail and in-application advertisements. Another popular adware application is the popular Eudora Free e-mail client. In return for using Eudora, users agree to accept advertisements. In many ways, all modern adware applications use a similar technique, although to questionably less benefit for the end user.



Eudora E-Mail Client

3.3 Spyware Applications

Unlike cookies, which were designed to improve the user's Internet experience, and the initial adware applications, which were intended to pay developers for the free distribution of their programs, the first spyware applications were designed to surreptitiously harvest and exploit user activities. Programs seeming too good to be true (including Napster, arguably) that were often bundled with nothing more than several pieces of spyware were the most common spyware infection vector. Actions taken during and after installation ranged from subtle to blatant, and the effects ranged from harmless to devastating.

Despite the actions taken or the consequences of those actions, initial spyware programs impeded the use of the computer on which it was installed. In many instances, spyware rendered computers inoperable, which under different circumstances would have been considered a local denial of service (DoS) attack. Entire computers required reformatting and reloading to thwart spyware and, in some cases, previously installed programs and/or valuable data was lost. Pop-ups and "pop-unders" that redirected users to offensive websites or websites with questionable material were prevalent, resulting in the creation of pop-up-blocking software.

While modern spyware tends to be more discreet than most of the early versions (sometimes even running in the background without detection), it can still harvest cookie information from all websites visited on the infected computer and deliver targeted advertising to users based on previous activity. Given all of this, it is no wonder that an entire industry has evolved that is devoted to the prevention and removal of spyware.

3.4 Advertising Motives

The history of spyware demonstrates that its primary function is delivering advertising to prospective customers. In fact, the *American Heritage Dictionary of the English Language, 4th edition*, defines the word "advertise" as:

> ***ad·ver·tise** (ăd'vər-tīz')*
> *v. ad·ver·tised, ad·ver·tis·ing, ad·ver·tis·es*
> *v. tr.*
> *1. To make public announcement of, especially to proclaim the qualities or advantages of (a product or business) so as to increase sales.*

Traditional advertising has long collected information about groups or individuals and directed advertising toward these demographics; an approach that maximizes return on investment for the advertiser.

Spyware, as designed and distributed by their authors, simply takes directed advertising one step further, directing it toward individuals instead of demographic samplings. However, in most cases, the responsibility for accepting advertising lies with users, which yields an alternate definition of advertising, this one coined by British-Canadian writer and economist Stephen Butler Leacock:

> *Advertising may be described as the science of arresting the human intelligence long enough to get money from it.*

Spyware demonstrates that suspending intelligence can be easily affected though deception, inveiglement and obfuscation. How exactly, then, does spyware advertising differ from traditional print, television, radio or billboard advertising? Quite simply, it does *not* differ, at least in its native form, from

traditional forms of advertising. As natively supplied or encountered, none of the top-10 spyware applications can be installed without user interaction; however, none of these spyware applications explicitly state the scope their actions. It must be noted, however, that legitimate programs (e.g., MSN Messenger or Microsoft Windows) do not fully state the scope of their actions, either. So, despite the hue and cry of many Internet "purists," advertising is here to stay, and practically every company website and every ISP website contains some sort of advertising.

Since spyware is not illegal in and of itself, it can be distributed by any imaginable means (legal or illegal). Websites, e-mail messages, removable media and legitimate programs can serve as the "infection" vector, and the installation can be as above-board as a legitimate application or as surreptitious as an Internet worm. The end result of "unauthorized" spyware installation is that a third party (i.e., the malicious spyware distributor) receives a piece of the pie. Through reimbursement programs, such as pay-per-click advertising, malicious spyware distributors, who are clearly unconcerned with the damage that they cause spyware companies, can defraud the system.

In fact, malicious spyware distributors have lately increased the number of innovative techniques by which they distribute spyware. One such attack exploited users who mistyped "google" as "googkle," resulting in malicious code droppers downloading and installing hundreds of auto-installation files that were a combination of malicious code and spyware applications (see ID# 411064, April 27, 2005, "Googkle Malicious Website Infects Visiting Computers"). Another attack, the Bestcounter.biz attack, used an in-line frame (iFRAME) element to exploit vulnerable computers (see ID# 208704, Nov. 25, 2003, "MS-ITS URL Handler Vulnerability") and profit from a spyware affiliate program (iframeDOLLARS.biz). Most recently, spyware wreaked havoc on users visiting an ever-growing list of websites that exploited the Microsoft Windows shimgvw.dll WMF File Handling Remote Code Execution Vulnerability (ID# 433984, Dec. 28, 2005) to install spyware without users' knowledge or permission.

3.5 Conclusion

Considering the innumerable means by which spyware can be distributed, spyware delivery to a targeted audience is virtually guaranteed.

4 Top-10 Spyware Threats

As 2006 begins, several anti-spyware companies are reporting the prevalence of different spyware applications. As a result, no two top-10 lists are the same. Webroot Software (http://www.webroot.com/resources/spywareinfo/threats.html) compiled the following list that incorporates the ten most common spyware threats:

Spyware Threat	Description
1. CoolWebSearch (CWS)	CoolWebSearch could hijack any of the following: Web searches, home pages and other Internet Explorer settings. Recent CoolWebSearch variants install using malicious HTML applications or security flaws, such as exploits in the HTML Help format and Microsoft Java Virtual machines.
2. Gator (GAIN)	Gator is an adware program that could display banner advertisements based on user web surfing habits. Gator is usually bundled with numerous free software programs, including the popular file-sharing program Kazaa.
3. 180search Assistant	180search Assistant is an adware program that delivers targeted pop-up advertisements to users' computers. Whenever a key word is entered into a search engine or a targeted website is visited, 180search Assistant opens a separate browser window that displays an advertiser's Web page related to the keyword or website.
4. ISTbar/AUpdate	ISTbar is a toolbar used to search pornographic websites and could display pornographic pop-ups and hijack user homepages and Internet searches.
5. Transponder (vx2)	Transponder is an IE Browser Helper Object (BHO) that monitors requested Web pages and data entered into online forms, then delivers targeted advertisements.
6. Internet Optimizer	Internet Optimizer hijacks error pages and redirects them to its own controlling server at http://www.internet-optimizer.com.
7. BlazeFind	BlazeFind could hijack any of the following: Web searches, home pages and other Internet Explorer settings. BlazeFind could redirect Web searches through its own search engine and change default home pages to www.blazefind.com. This hijacker could also change other Internet Explorer settings.
8. Hot as Hell	Hot as Hell is a dialer program that dials toll numbers to access paid pornographic websites. Hot as Hell may disconnect computers from a local Internet provider and reconnect it to the Internet using an expensive toll or international phone number. It does not spy on the user, but could accrue significant long distance phone charges. It might run in the background, hiding its presence.
9. Advance Keylogger	Advanced Keylogger can monitor keystrokes and take screenshots.
10. TIBS Dialer	TIBS Dialer is a dialer that could hijack a modem and dial toll numbers that access paid, pornographic websites.

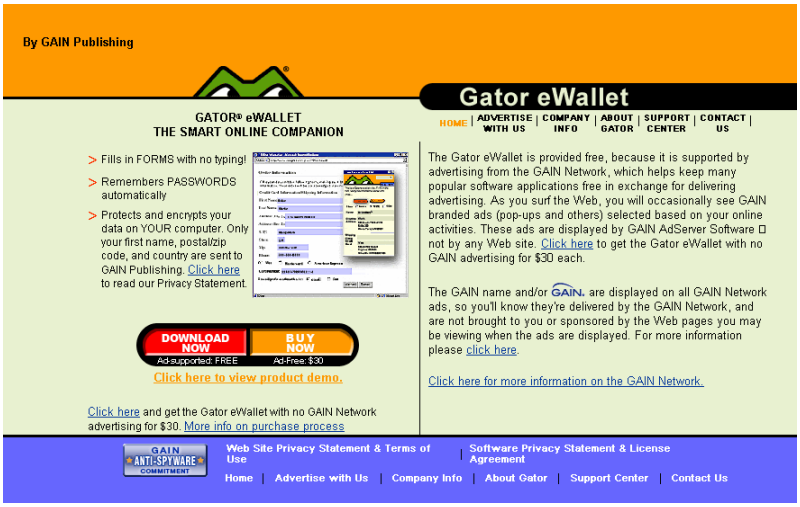
While each of these spyware applications differs in functionality, they have the following commonalities:

- They fit the iDefense definition of spyware
- They are all legal products under current legislation
- They all obfuscate their installation and presence
- They all result in financial gain to their companies
- They can be installed via malicious code techniques
- They can cause substantial performance degradation
- They can result in data integrity issues

5 Typical Spyware Installation

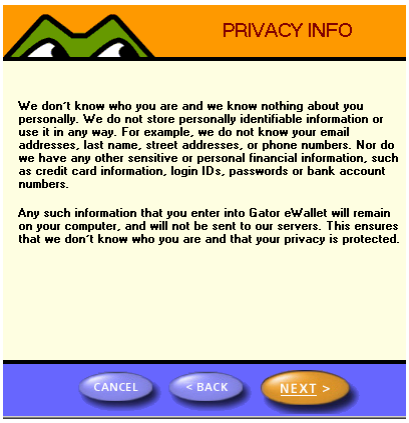
Most spyware available to advertisers today follow industry-accepted guidelines for installation and removal. Typically, users must download an executable file promising the functionality sought, then opt to install the program and agree to the spyware End-User License Agreement (EULA). It is in this legally-binding EULA, not the promotional websites, e-mail messages or installation screens, where the application's true intent can be determined.

An excellent example is the Gator eWallet. Gator eWallet is supposed to help users tired of the hassles involved in making online purchases (i.e., filling out repetitive forms, remembering passwords, etc.). So, targeting such users, Gator distributes the following e-mail message containing a link to the eWallet information and download page:



Gator eWallet Overview Page

Someone interested in such a product receives the e-mail and visits the Gator eWallet Web page. The information found on this page indicates that Gator eWallet will, indeed, meet the user's needs and the user proceeds to install the application. During each step of the installation, a new screen with new text and information is presented, along with the "next" button to continue. On the sixth screen, a seemingly reasonable privacy statement is displayed:



Gator eWallet Privacy Statement

On the seventh screen, the Privacy Statement and EULA are displayed, which the user must certify has been read. Once read, the user must accept the agreements to proceed with the installation:

Gator eWallet Privacy Statement and EULA Acceptance

To recap, the user has found an application (Gator eWallet) that will make it easier to make online purchases and has read the privacy page stating that Gator does not store "personal" information – a page that is conveniently well-nested in the installation process (i.e., six screens into the process). However, only the Privacy Statement and EULA, which are six pages long and worded in legalese, fully explain the actions taken when Gator eWallet is installed. For example:

> "**What Information Does GAIN Collect?**
> GAIN Is Designed to Collect and Use Non-Personal Information. GAIN collects certain non-personally identifiable information about your Web surfing and computer usage. This includes the URL addresses of the Web pages you view and how long you view Web pages; non-personally identifiable information on Web pages and forms including the searches you conduct on the Internet; your response to online ads; Zip code/postal code; country and city; standard web log information and system settings; what software is on the computer (but no information about the usage or data files associated with the software); software usage characteristics and preferences; and, for Gator(R) eWallet users, your first name and master password, if you choose to create one. For more information regarding the data we collect, click: www.gainpublishing.com/rdr/70/datause.html."

(**NOTE**: The entire six-page agreement is included in Appendix 1.)

After reading the full privacy statement and EULA, it is clear that installation allows for far more invasive action on the publisher's part than any of the installation screens state. Indeed, the installation screens certainly do not mention that the user's Internet browsing will be impeded by the product, that users' interests will be logged so that they may be directly targeted by advertisers, that Gain Advertising Search Scout will interfere with users' link selections or that eWallet will install more than 150 files to the user's computer and make more than 155 Windows Registry entries. Nor do these screens state that Gain advertising is installed as a separate component and, therefore, remains installed even when eWallet is uninstalled.

6 Obfuscation of Actions

Reviewing once again the iDefense definition of spyware, it can be seen that the previous example (and most other spyware analyzed to date) obfuscates the intended action of the spyware from the end user by including it in a massive document; typically the true action is included in the multi-page EULA and not on the installation screens or product information page. It is doubtful that everyone always reads the EULA completely before installation – for instance, how many know that MSN Messenger cannot be used for business purposes without express written permission from Microsoft? When it comes to the obfuscated actions of spyware, then, the acceptance of the EULA to continue with the software installation is not explicit, but implicit.

The actual action performed by the spyware is also in compliance with our definition. Despite a disclosure on the installation screen that no personal information is tracked, actual browsing patterns are tracked and recorded, allowing the spyware application to customize advertising to the end user.

7 Legitimate Spyware?

In a post made to its website on (a copy of which is included in Appendix Two), Cool Web Search boldly proclaims that its software is for legitimate purposes only. Other adware companies, such as the one that distributes the well-known "Gator" product (currently the Claria Corporation, http://www.claria.com), have historically threatened libel law suits against companies claiming that the Gator product is spyware (news.com.com, Oct. 22, 2003, http://news.com.com/2100-1032_3-5095051.html?tag=techdirt), because, after all, the end user must accept (the six page) electronic EULA to install Gator.

In a more recent case, anti-spyware software firms such as Aluria, Lavasoft and PestPatrol were forced to remove detection for spyware distributed by some companies (such as Claria and WhenU), a process known as "delisting." Whether the delisting occurred because of petitioning or because of legal cease-and-desist orders, the end result is the same - products produced by those companies are no longer detected in anti-spyware scans (PCWORLD.com, May 31, 2005, http://www.pcworld.com/news/article/0,aid,120914,00.asp). It should be noted that the link to this article (and perhaps the article itself) has been removed by *PC World*.

Of course, the word spyware itself is viewed as derogatory by its distributors, so some security companies are now referring to spyware as "grayware" or simply by the description of "potentially unwanted software." The crux of the problem is that both sides of the spyware/anti-spyware conflict engage in legitimate and successful business practices, and that those left in the middle – the computer users - are effectively paying both sides for the privilege to use their computers and the Internet.

8 Legislative Anti-Spyware Efforts

On Feb. 27, 2004, Senator Conrad R. Burns (R-MT) introduced the Software Principles Yielding Better Levels of Consumer Knowledge (SPY BLOCK) Act (see http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02145). This bill did not ban spyware, but regulated the manner in which such applications can be installed and the functions they can perform after installation. The bill did not, however, define spyware, and this alone may have adversely impacted the bill's efficacy.

SPY BLOCK specifically prohibits:

- Installing software without notice to and consent from the user
- Installing software without an available and proper un-installation option
- Misleading the user about who is responsible for the program or the services that it provides
- Not taking reasonable measures to protect users' privacy

On May 24, 2005, two bills passed the U.S. House of Representatives and were sent to the U.S. Senate for review: the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) and the Internet Spyware Prevention Act (I-SPY Act) (see http://www.pcworld.com/news/article/0,aid,120985,00.asp).

While these prohibitive actions are a good start, there is still sufficient wiggle-room for spyware companies to circumvent the consequences of violating the bill's purpose. The fact that SPY BLOCK has been in congress for more than one year without being passed speaks volumes about its likely success after passage.

Similar trends can be seen in the ineffectiveness of the CANSPAM Act.

9 Spyware Mitigation Strategies

9.1 Attitude and Policy

It is not uncommon for corporate security personnel to employ a highly stringent policy toward the computers on the networks for which they are responsible. In fact, many corporate security personnel view spyware as a de facto type of malicious code, and have extended their existing malicious code policies to spyware itself, at least as far as the corporate network is concerned. Unfortunately, due to the fact that spyware comes in many flavors and its methods of installation are constantly evolving, it is often difficult for the individual end user to comply with the stringent policies, especially in an age of access to centralized resources through remote connectivity.

9.2 Workstation and User Restrictions

Many corporate networks limit or eliminate a user's ability to install new programs on specific workstations. These user and/or computer restriction policies "lock down" a computer so that it may only execute in a predefined state, and can only run pre-approved applications. This is a solid and respectable means of avoiding most malicious code and spyware.

With the integration of Web-based application capability into the operating system, however, increasing numbers of malicious code and spyware applications are subverting these protections, forcing security personnel to choose between a fully locked-down computer and a functional computer.

9.3 User Education

User education on computer security related topics has invariably met with mixed results. This is demonstrated by the increase in successful social engineering malicious code attacks, in which the end user must take overt action for the infection to begin. If education were indeed the sole solution to computer security issues, social engineering attacks would have ceased long ago. Instead, social engineering is still the most widely used attack vector, not only for malicious code, but also for spyware, spam and phishing attacks.

Despite this, user education can still play a vital role in mitigating the spyware menace; it does not hurt to inform users of the risks and consequences involved in inappropriate behavior.

10 Signature-Based Scanning Solutions

One of the most popular ways to mitigate the spyware threat is through the use of signature-based scanning solutions similar to anti-virus software. This technological approach to controlling the spyware problem is increasing, with more than a dozen "major" players and scores of "minor" players vying for a piece of the monetary pie. In fact, it is estimated that the number of installations for signature-based spyware solutions will increase to 540 million seats by 2009 (The Radicati Group, http://www.radicati.com/cgi-local/brochure.pl?pub_id=511&subscr=&back_link=/reports/single.shtml, June 2005).

This growth represents an approximate 30-fold growth in the current number of installations, and is illustrative of the growth of the spyware problem and the increasing impact of spyware on the confidentiality, integrity and availability of computing resources.

The following sections discuss several types of products that currently exist for detecting, preventing installation of, and removing spyware.

10.1 Traditional Anti-Virus Solutions

As a further testament to the blurring lines between malicious code and spyware, many spyware programs are now being installed by malicious code and malicious code tools such as droppers and downloaders. An excellent example of this approach to spyware distribution is documented in the iDefense report, "WarSpy.B Trojan Horse Compromises Computer Security" (ID# 415072, June 30, 2005). The WarSpy.B Trojan horse dropped the following shortcuts to the infected user's desktop:

- Air Tickets.url
- Big Tits.url
- BlackJack.url
- Britney Spears.url
- Car Insurance.url
- Cigarettes.url
- Credit Card.url
- Cruises.url
- Forex Trading.url
- Lesbian Sex.url
- MP3.url
- Online Betting.url
- Online Casino.url
- Oral Sex.url
- Party Poker.url
- Pharmacy.url
- Phentermine.url
- Pornstars.url
- Remove Spyware.url
- Viagra.url

10.2 Dedicated Anti-Spyware Solutions

Dedicated software designed to detect and eliminate spyware is one of the fastest-growing IT markets today. Dedicated anti-spyware solutions are becoming increasingly proficient at detecting and eliminating spyware applications through signature-based scanning. Two sites, Anti-Spyware Software Review (http://anti-spyware-review.com/) and Adware Report (http://www.adwarereport.com/) provides overviews and comparisons of the most popular commercial anti-spyware products. A comparison of the two "top 10" lists yields dramatically different testing results, and therefore the listings should be used more as a guideline than as a rule. Also, while the sites claim independence, the exact nature of their independence could not be determined.

10.3 Hybrid Anti-Virus/Anti-Spyware Solutions

With the increased threat from spyware, some traditional anti-virus companies are getting into the act and adding spyware signatures to their existing anti-virus solutions. While this may seem like the optimal approach, none of the hybrid products offered to date is as comprehensive as are the best dedicated anti-spyware solutions.

10.4 Problems with Signature-Based Scanning Solutions

The downside of all of anti-spyware scanning solutions is that they rely primarily upon signature-based technologies, and the development of anti-spyware (or anti-virus) signatures always lags behind the release of a new spyware threat, no matter how severe that threat may be.

Signature-based scanning solutions must include signatures for specific spyware threats, and the distributors of the spyware may take exception to being categorized as such and threaten litigation. The threatened litigation may result in a temporary (or permanent) delisting of the spyware product from various signature-based scanner vendors, and the end-user is unlikely to know when this occurs, leaving them vulnerable (PCWORLD.COM, http://p144.news.scd.yahoo.com/s/pcworld/20050623/tc_pcworld/121583, June 23, 2005). The delisting process is particularly a problem with smaller companies lacking the financial resources to defend themselves from the actions of large spyware distributors.

Another problem is that anti-spyware vendors may intentionally form partnerships with particular spyware distributors. A recent example of this is Microsoft's partnership with the infamous Hotbar.com, as reported on the Adware Report website (http://www.adwarereport.com/mt/archives/000150.html, June, 2005). In fact, upon visiting http://www.hotbar.com, the Microsoft Partnership logo is proudly displayed:

Microsoft Certified Partner Logo on Hotbar.com

The corresponding partner profile can be located at: http://directory.microsoft.com/mprd/PartnerProfile.aspx?RowKey=b0d237a7-3fc8-411f-862f-d8dd15dfb599&LanguageDropDown=173.

An excerpt of this partner profile follows:

Partner Profile

HOTBAR.COM INC

(HOTBAR.COM INC.)

Hotbar.com, Inc. is a New York City based Internet company dedicated to customizing and maximizing the Web's interactive potential. Founded upon a vision to change the way people browse the Web, Hotbar.com developed the patent pending Hotbar Smart Toolbar, a revolutionary browser add-on that brings the entire Internet to the browser. This Smart Toolbar categorizes over 2.5 million sites into over 2,000 major categories and over 200,000 sub-categories. While surfing, the toolbar's Smart Buttons relate to each particular site visited, offering additional information on the related topic.

Microsoft CERTIFIED Partner

This description and profile was provided verbatim by the partner

HOTBAR.COM INC
HOTBAR.COM INC.
226 West 37th St. (11th floor)
New York
New York
10018
United States

Hotbar.com Partnership Profile in Microsoft's Partner Directory

The previously described delisting fiascos and the Microsoft/HotBar partnership have eroded confidence in some of the anti-spyware vendors, and in Microsoft's case has led to allegations of the "fox guarding the henhouse," even though Microsoft anti-spyware currently detects HotBar as a spyware application. It is obvious that industry-wide effort must be exerted on standardizing what specific applications should be considered as spyware.

11 Intelligence Information

Spyware intelligence provides timely and actionable information on emerging spyware threats, often before anti-virus and/or anti-spyware software companies can develop signatures for the threats. Two recent iDefense Intelligence Operations reports, *DLoader.PT Trojan Horse Downloads and Executes Malicious Code* (ID# 413703, June 7, 2005) and *RBot.BDB Worm Propagates via Weak Network Shares* (ID# 415000, June 29, 2005), are examples of spyware being distributed by malicious code that was undetected by the major anti-virus vendors. Clearly, then, advanced intelligence can assist in spyware mitigation.

11.1 Gateway Anti-spyware Products

Analogous to gateway anti-virus solutions, there are several emerging gateway anti-spyware products that promise to stop spyware before it enters the network. While no comprehensive independent reviews are available for these anti-spyware gateway products, PCMag.com tested the efficacy of gateway anti-virus products and found that they were not 100 percent effective (PCMAG.COM, http://www.pcmag.com/article2/0,1895,1600557,00.asp, June 8, 2004). Considering that the techniques for detecting and preventing malicious code and spyware are very similar, it is reasonable to assume that the response of a gateway anti-spyware product is similar to gateway anti-virus products.

12 Conclusion

Computer users in well-protected corporate networks are less likely to fall victim to spyware than are home users. However, in a society marked by an increasingly mobile workforce, spyware threats must be taken seriously. As anti-spyware solutions are not completely effective (see Keizer, Gregg, "Desktop Anti-Spyware Doesn't Cut It, Survey Says," *InformationWeek*, March 14, 2005, http://informationweek.com/story/showArticle.jhtml?articleID =159402838), and as advertising companies increasingly employ new techniques to increase profitability, corporations must reexamine the spyware threat and their response procedures.

Additionally, postings to independent newsgroups indicate that the spyware problem is not confined to home users, but that it often spills over into the corporate world, costing businesses time and money. The fact that major anti-spyware companies are being coerced into delisting particular products indicates the level of intensity of the current problem.

As the spyware threat increases, so will the expenditures to combat the threat. Despite the legislation with which corporations must comply, there is no legislation currently in effect to help them stave off the spyware threat. Distribution methods currently employed by spyware authors and distributors, while deceptive, do not violate the letter of the law. In addition, these techniques don't even violate restrictions included in the proposed SPY BLOCK legislation.

Even with the above prohibitions, it is obvious that much of the available spyware (such as Gator eWallet) is not in violation.

Even if legislation does change to better address adware and spyware issues today, a cat and mouse game will likely continue. Adware and spyware authors will quickly change the manner of installation and craft EULAs to get around whatever legal barriers put in place by the revised legislation.

Corporations must therefore fend for themselves when confronting the spyware threat, following industry best-practices coupled with technology-based mitigation strategies.

Appendix 1 - Gator EULA Agreement

--- Privacy Statement and End User License Agreement ---

You must agree to the terms of this Privacy Statement and End User License Agreement before you may install GAIN-Supported Software (defined below).

In exchange for offering you free software products, we collect anonymous usage information from your computer that we and our partners may use to select and display pop-up and other kinds of ads to you and to perform and publish research about how people use the Internet.

--- GAIN PRIVACY STATEMENT ---

What is GAIN?
GAIN Publishing offers some of the most popular software available on the Internet free of charge ("GAIN-Supported Software") in exchange for your agreement to also install GAIN AdServer software ("GAIN"), which will display Pop-Up, Pop-Under, and other types of ads on your computer based on the information we collect as stated in this Privacy Statement. We refer to consumers who have GAIN on their system as "Subscribers."

What Information Does GAIN Collect?
GAIN Is Designed to Collect and Use Non-Personal Information. GAIN collects certain non-personally identifiable information about your Web surfing and computer usage. This includes the URL addresses of the Web pages you view and how long you view Web pages; non-personally identifiable information on Web pages and forms including the searches you conduct on the Internet; your response to online ads; Zip code/postal code; country and city; standard web log information and system settings; what software is on the computer (but no information about the usage or data files associated with the software); software usage characteristics and preferences; and, for Gator(R) eWallet users, your first name and master password, if you choose to create one. For more information regarding the data we collect, click: www.gainpublishing.com/rdr/70/datause.html.

If you voluntarily submit personally-identifiable information to us - for example, when you request technical support - we only use that information to respond to you or handle your request. We do not merge it with the information collected by GAIN.

How Do We Use This Information?
- To Deliver GAIN Ads. GAIN Publishing associates the non-personally identifiable information that GAIN collects to an anonymous, randomly generated Subscriber ID to create a profile of the categories of products or services in which Subscribers appear to be interested. We may also use information we collect to infer certain Subscriber demographic information such as gender, age range, and marital status.

We use the information we collect to display relevant ads on your computer ("GAIN Ads"). For representative full size examples of the each type of GAIN Ad that we may display and for ad vehicle frequency information, click: www.gainpublishing.com/rdr/70/about.html.
GAIN Ads will appear while you are browsing the Web, not just when you use GAIN-Supported Software. GAIN Ads are not usually associated with or sponsored by the website that you are viewing at the time you receive them. In fact, GAIN Ads may be from a competitor of a website you are viewing.

All GAIN Ads have the GAIN logo or "GAIN" in the title bar so that you will know that they were displayed by us. All of our Pop-Up ads also have a "?" in the upper right-hand corner and/or a "more info" link at the lower right hand corner. Clicking on either of these icons will provide you with more information about GAIN Ads and how to uninstall GAIN from your computer.

- To Enhance Third-Party Advertising.
We may also develop commercial relationships with third-party websites ("Third Party Advertising Partners") to make the ads you are shown more relevant to you when you view their websites. We do this through the use of your anonymous behavioral profile and demographic inferences. If you would like to know your choices about having your anonymous information used in this way, click: www.gainpublishing.com/rdr/70/cookies_out.html.

- To Conduct Research.
We aggregate anonymous data regarding Subscribers' online activities to better understand how consumers use the Web. For example, we may gather and use information on how Subscribers use various search engines or websites.

With Whom Do We Share Information?
- Search Partners.
We may transmit our Subscribers' search queries to search partners, who use this information to provide us with search results and other information, which we then display to our Subscribers.

- Third-Party Advertising Partners.
We may share information we collect with our Third Party Advertising Partners. If we do so, we will require by contract that they treat this information in accordance with our privacy promises.

- For Research.
We use aggregate anonymous data regarding Subscribers' online behavior to better understand how consumers use the Web. To that end, we may use aggregated, anonymous online traffic behavior to report emerging Web usage trends to the press or to the public. For example, we might issue a press release stating that GAIN Subscribers tend to visit certain websites more often than others. We may also use this aggregated, anonymous information to develop reports for our corporate clients so that they can better understand trends in online consumer behavior and how those trends relate to their businesses.

- Other Limited Circumstances.
We may also share information with third parties who help us perform a business function (their use of such information is limited by our internal policies and/or confidentiality agreements, as applicable); to protect our rights, or if under a legal obligation. For more information, click: www.gainpublishing.com/rdr/70/disclosure.html

Cookies and Web Beacons
Claria may write and access cookies on your computer. Among other things, these cookies enable us, or our Third Party Advertising Partners, to use anonymous behavioral profiles and demographic inferences to increase the relevance of online ads you receive.

Some GAIN Ads include "web beacons," and some of our advertisers and Third Party Advertising Partners may also include web beacons on some of their web pages at our request. These web beacons allow us to access the cookies we set and provide ad campaign analysis. For more information on cookies and web beacons, click: www.gainpublishing.com/rdr/70/cookies.html.

How Do I Stop The Display of GAIN Ads?
You can stop receiving GAIN Ads by uninstalling all of the GAIN-Supported Software from your computer, or, alternatively, purchasing a license to ad-free versions of all GAIN-Supported Software on your computer where available. Because the use of GAIN is required as long as you keep a copy of one or more, GAIN-Supported Software products on your computer, GAIN cannot be independently uninstalled. The only authorized means to uninstall GAIN-Supported Software is to use the Add/Remove Programs facility in the Microsoft Windows Control Panel. To see which GAIN-Supported Software is on your computer, and for more detailed uninstall instructions, click: www.gainpublishing.com/rdr/70/about_gain.html. After the removal of all GAIN-Supported Software, GAIN will immediately cease the display of advertisements, and will automatically remove itself from your computer, typically within a few minutes.
If you have any trouble removing our software, of if you have other questions about GAIN, click: www.gainpublishing.com/rdr/70/contact.html to send us an e-mail or get our toll free telephone number.

Some of our GAIN-Supported Software has ad-free versions available for purchase. If you purchase any such software, you will not receive GAIN advertising (unless you have other, free versions of GAIN-Supported Software), but GAIN will collect and use the anonymous information described in this privacy policy. To purchase versions of our GAIN-Supported Software that do not display advertising click: www.gainpublishing.com/rdr/70/software.html.

Sale, Merger, or Asset Transfer
If Claria Corporation or any of its assets is purchased or merged with another company, information we have collected from you may be one of the transferred assets.

Changes to this Statement
If Claria (or its successors) makes any material changes to our collection, use, or disclosure of your personally identifiable information, we will give you notice of these changes (such as by using an online pop-up message) and an opportunity to choose whether to have your personally-identifiable information treated under the terms of the revised policy. We will also continue to publish the current Privacy Statement on our website.

For support questions contact us at support@gainpublishing.com. For specific questions regarding the specific terms of this Privacy Statement, contact us at privacy@gainpublishing.com.

--- GAIN PUBLISHING END USER LICENSE AGREEMENT ---

The capitalized terms in this GAIN Publishing End User License Agreement ("Terms") shall have the same definitions provided in the GAIN Publishing Privacy Statement ("Privacy Statement"). GAIN and GAIN-Supported Software shall be collectively referred to as "Licensed Materials." In order to install any Licensed Materials, you must agree to these Terms. Installation and use of the Licensed Materials is voluntary and you may terminate these Terms at any time by uninstalling all GAIN-Supported Software using the Microsoft Windows Add/Remove Programs function. For more detailed uninstall instructions, click: www.gainpublishing.com/rdr/70/about_gain.html. Likewise, we may modify or discontinue your right to access or use the Licensed Materials at any time and for any reason.

- Ownership and Authority to Bind Users of Subscribers' Computers.
You must either own the computer on which the Licensed Materials will be installed, or you must be authorized by the owner of the computer to install it. If the computer has other users, you must obtain their consent to these Terms.

- Scope of License and License Restrictions.
Solely for your own personal, non-commercial purposes, we grant you the right to install the Licensed Materials and use GAIN-Supported Software. These are your only rights with regard to the Licensed Materials. The Licensed Materials are licensed, not sold to you. You may not modify, reverse-engineer, decompile, disassemble, or otherwise discover the Licensed Materials. All communications between GAIN Publishing and the Licensed Materials and the content stored on GAIN Publishing's computer servers and in the Licensed Materials includes confidential information of GAIN Publishing and you may not access, publish, transmit, display, create derivative works of, store, or otherwise exploit any such confidential information except as such functions are performed by the Licensed Materials in the ordinary course of operation. You do not have the right to create derivative works of Licensed Materials.

- Interference.
You agree that you will not use, or encourage others to use, any method to uninstall the Licensed Materials other than through the use of the Add/Remove Programs feature of the Microsoft operating system. Use of any robot, spider, other automatic or non-automatic manual device or process intended to interfere or attempt to interfere with the proper working of the Licensed Materials is prohibited.

- Privacy.
The Privacy Statement is incorporated into these Terms. Our Privacy Statement governs the collection, use and disclosure of information we collect from you. Users of the Gator eWallet, are solely responsible for maintaining the confidentiality of their Gator eWallet master password. They are also responsible for all uses of their Gator eWallet master password and any and all related uses of their information stored in any GAIN-Supported Software.

- Updates.
Occasionally, we may, automatically, or through other means, update, upgrade, or patch the Licensed Materials. Your license to an existing version of Licensed Materials may, at GAIN Publishing's discretion, expire when new versions of Licensed Materials are released. Notwithstanding the foregoing, we have no obligation to make available to you any subsequent versions of Licensed Materials.

- Disclaimer of Warranty.
USE OF THE LICENSED MATERIALS IS AT YOUR OWN RISK. GAIN PUBLISHING PROVIDES THE LICENSED MATERIALS ON AN "AS IS," "WHERE IS," BASIS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, OR NON-INFRINGEMENT. GAIN PUBLISHING ALSO DISCLAIMS ALL LIABILITY WITH REGARD TO YOUR VIEWING OF ANY WEB PAGES THAT MAY BE AVAILABLE BY LINK OR OTHERWISE FROM SEARCH RESULTS OR OTHER INFORMATION YOU RECEIVE WHEN USING GAIN-SUPPORTED SOFTWARE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT. GAIN PUBLISHING MAKES NO WARRANTY THAT INFORMATION PROVIDED BY THE LICENSED MATERIALS IS ACCURATE, RELIABLE, TIMELY, UNINTERRUPTED, ERROR-FREE, OR OTHERWISE WILL MEET YOUR EXPECTATIONS. THE ABOVE EXCLUSIONS MAY NOT APPLY IN JURISDICTIONS THAT DO NOT ALLOW THE EXCLUSION OF CERTAIN IMPLIED WARRANTIES.

- Limitation of Liability.
IN NO EVENT WILL GAIN PUBLISHING, CLARIA, DISTRIBUTORS OF THE LICENSED MATERIALS, SUPPLIERS, ADVERTISERS, OR THIRD PARTY DEVELOPERS, OR ANY OF THE FOREGOING ENTITIES' OFFICERS, DIRECTORS, EMPLOYEES, OR AGENTS (COLLECTIVELY "Protected Parties") BE LIABLE FOR ANY INDIRECT DAMAGES, INCLUDING, BY WAY OF ILLUSTRATION AND

NOT LIMITATION, LOST PROFITS, LOST BUSINESS OR LOST OPPORTUNITY, OR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING LEGAL FEES, ARISING OUT OF THE DOWNLOAD, USE, OR INABILITY TO USE THE LICENSED MATERIALS, OR INFORMATION YOU RECEIVE WHEN USING THE LICENSED MATERIALS. IN NO EVENT WILL THE MAXIMUM CUMULATIVE LIABILITY UNDER THESE TERMS, OR THE GAIN PUBLISHING PRIVACY STATEMENT, EXCEED THE LESSER OF $100 OR THE REVENUE ACTUALLY RECEIVED BY GAIN PUBLISHING OR CLARIA DIRECTLY ATTRIBUTABLE TO YOUR USE OF THE LICENSED MATERIALS.

Because some states or jurisdictions do not allow the exclusion or the limitation of liability for consequential or incidental damages, in such states or jurisdictions, the Protected Parties' liability shall be limited to the extent permitted by law.

- Compliance with Laws.
You must comply with all applicable laws, including export control laws, and these Terms. For more information on compliance with export laws, click: www.gainpublishing.com/rdr/70/export.html. Some states may restrict or regulate your use of the Licensed Materials. Click: www.gainpublishing.com/rdr/70/stateregs.html for more information on this topic. We may display important messages to Subscribers in certain regions or States and may use your computer's time zone settings to determine which Subscribers should see such messages. To ensure that you receive those messages, you hereby represent that your computer's time zone settings accurately reflect the physical location of your computer.

- Applicable Law.
The laws of the State of California will govern these Terms, without reference to conflicts of law principles. The United Nations Convention on Contracts for the Sale of Goods does not apply to these Terms.

- Arbitration.
Any claim or controversy arising out of or related to these Terms, the Privacy Statement, or the Licensed Materials shall be settled by binding arbitration in San Mateo County, California, in accordance with the rules of the American Arbitration Association. Any such claim or controversy shall be arbitrated on an individual basis and shall not be consolidated with a claim of any other party. The foregoing shall not preclude GAIN Publishing from seeking any injunctive relief in State or Federal courts for protection of its intellectual property rights.

- General.
These Terms set forth the entire understanding and agreement between you and us with respect to the subject matter hereof. If any provision or provisions hereof shall be held to be invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remaining provisions shall not be in any way affected thereby. Except as described herein, you may not assign these Terms without our explicit consent. These Terms may change in the future. In such case, and when appropriate, GAIN Publishing will obtain your consent prior to the new Terms. You are responsible for fees associated with gaining access to the Licensed Materials, including the fees associated with the equipment necessary to access the Internet and the fees charged by your ISP.

GAIN Publishing, the GAIN Network, and Feedback Research are business units of the Claria Corporation. Microsoft Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Effective December 2004

Appendix 2 - CoolWebSearch Defense Post

News Update (2005-08-09):

As you may have heard, there is a new spyware identity theft ring out there:
http://news.yahoo.com/s/zd/20050808/tc_zd/157623
http://sunbeltblog.blogspot.com/

For some obscure reason, they keep claiming that it has something to do with coolwebsearch. It does not. We urge anyone who has any evidence on this actually being linked to us to come forward and let us know. If one of these people is actually working for us, we will contact the FBI and release his information immediately. In addition we will of course close his account and withhold his or her payment for violation of our rules, as we have done with all the so called "hijackers."

Our lawyers are currently thinking of suing yahoo and all the other places who posted this article with "CoolWebSearch" in it as the name of the so called exploit for slander. Please get your facts straight before doing these things.

For reference purposes, this is how you find out whether or not a website is related to coolwebsearch: you click a link and you track where the redirections go. If it goes through the CWS IP, which is currently 66.250.74.152, or the domain coolwebsearch.com then it is CWS, otherwise, IT'S NOT! There are dozens of hijacker outlets out there, and they are all called "CoolWebSearch" by those who do not bother to check their facts before posting articles on news sites.