Spyware: A Growing Software Threat

Dr. Thawar T. Arif
Assistant Prof. – MIS Department
Al-Isra Private University
Email: thawart@yahoo.com
Fax: +962-6-4711505

Abstract

Spyware is a kind of software installed by a third party without the user’s fully informed consent; it tracks the infected computer activities and sends the information to a spymaster. Spyware slows a machine over time and after repeated activities, the longer the time, then the worse performance likely becomes. It is indeed a threat to computer security, and yet the sort of maladaptive software application.

Spyware is more than an Internet nuisance. At the very least, it is an abuse of public trust by marketers, at the worst, a computer crime that can inflict real financial damages and uncertain legal consequences to individuals and organizations.

In this paper, the spyware phenomenon is surveyed. The reasons for spyware existence, how it can be detected, the violations and threats caused by spyware applications, have been discussed in some details. The spyware applications are classified in terms of behaviors, performance, and functions. Also, the steps for avoiding and solving the spyware problems are stated.

I- Introduction

Over the past few years, a relatively new computing phenomenon has gained momentum; that is the spread of spyware. Although there is no precise definition, the term “spyware” is commonly used to refer to software that, from a user’s perspective, gathers information about a computer’s use and relays that information back to a third party. This data collection occurs sometimes with, but often without, the knowing consent of the user [1].

Spyware belongs to the class of technologies that have emerged as a problem, a threat, a “disease,” as compared to the traditional technologies intended to be beneficial to organizations and individuals [2]. Spyware can also detract from the usability and
stability of a user’s computing environment, and it has the potential to introduce new security vulnerabilities to the infected host. Because spyware is widespread, such vulnerabilities would put millions of computers at risk [1].

Spyware resides on computers, tracking users’ movements on the Web, and hijacking Web browsers. It monitors a user’s online activities and triggers unwanted advertisement displays. Spyware represents one of many plagues on the Internet, comparable to spam and viruses. Spyware is also devious as it resides on a personal computer without the user’s knowledge. The nature of spyware contributes to unfair information practices, yet many consumers do not even realize its existence and the harm it can impart. As a result, they do not take appropriate procedures to protect their privacy [3].

Spyware is often introduced to a user’s system embedded within another software package such as a file sharing application, an instant messenger or another network dependent program. When the user installs the package the spyware is installed as well and starts gathering and sending personal information in one form or another. It is therefore often hard, even for experienced users, to distinguish between what is normal, intended, communication and what is spyware related [1, 4].

In the rest of this paper, the reasons for spyware existence are discussed in part two. In part three, most significant signs of spyware infections are stated. The threats imposed by spyware applications have been explained in part four. Also, the spyware violations are explained in part five. In part six, spyware applications are classified in terms of behaviors, performance and functions. In part seven, the most well-known examples of spyware are reviewed. The steps for avoiding and solving the spyware problems are stated in part eight.

II- Why Does Spyware Exist?

Spyware exists because information has value. For example, information gathered about the demographics and behavior of Internet users has value to advertisers, the ability to show advertisements correlated with user behavior has value to product vendors, and gathering keystrokes or introducing backdoor vulnerabilities on a host has value to attackers. As long as this value exists, there will be incentive to create spyware programs
to capitalize on it. Marketers use spyware to collect users’ buying information so that personalized marketing messages can be delivered to the users [1, 3].

Web users may perform some activities that unknowingly cause spyware to be loaded on their computers. The main sources of spyware infections are pop-ups, free downloads, and shareware. Some spyware has the capability of recording everything users type such as user names, passwords, and credit card numbers. Spyware can take control of the user’s browser, display unwanted ads, collect confidential information, redirect users to erroneous Web sites, and even monitor Web user’s behavior for potentially malicious purposes [3].

Spyware succeeds because today’s desktop operating systems make spyware simple to build and install. Operating systems and applications are designed to be extensible, and as a result, there are numerous interfaces for interposing on events and interacting with other programs. Operating systems also tend to hide information about background activities to shield users from unwanted complexity. The combination of these two properties makes it difficult to prevent spyware programs from gathering the information they want, or for the user to detect when such information is being harvested or transmitted [1].

Some of the main correlations that were found between spyware infected clients were that they also frequently visit many web sites, download executable files and download peer-to-peer file-sharing software. Visiting a lot of web sites seems to have a clear link to the degree of infection. The reason for this is assumed to be that being exposed to a lot of different web sites also makes the risk greater of encountering ones infested by malicious spyware code [4].

III- Signs of Spyware Infection:

It is estimated that 90% of all computers on the Internet are infected with spyware. Some telltale signs of spyware infection are [5-11]:
1) The infected computer slows to a crawl due to several spyware programs using up its memory resources.
2) A click on a link to go to one site, ends up at another site.
3) The infected computer is dialing up numbers on its own that show up on the user’s phone bill.
4) When the user enters a search item, a new and unexpected site handles the search.
5) The user click his Home button but it takes him to a new site, and when he switches the setting back, the new site appears again anyway.
6) The user gets pop-up advertisements that address him by name even when he has not visited site at which he has registered.
7) The user is subject to endless pop-up windows.
8) Advertisements pop up even when the infected computer is offline.
9) Unexpected toolbars appear in the user web browser.
10) Unexpected icons appear in the task tray at the bottom of user’s screen.
12) Certain keys fail to work in user’s browser (e.g. the Tab key doesn’t work when the user is moving to the next field within a form).
13) Slowing programs, shutting down computer, interfering with Internet.
14) Certain programs wouldn’t open.
15) Caused Internet Explorer to not function correctly.

The Anti-Spyware information webpage SpywareGuide.com has put together a 10-step list of how to monitor one’s system and check for the signs of spy software [12, 13]:

1. Work environment: Assume you are being monitored. Most workplaces have the right to do this so by default get used to the fact that someone is monitoring you. There are several ways employers can monitor employees. Some use activity logging software to see what programs are being accessed and for how long. Naturally many will use spy software programs also known as snoop ware or a key logger to take snapshots and log all keystrokes. An employer may actually monitor internet traffic as it moves across an intranet.

2. Anti-Spy programs: A popular way to find out if someone is spying on you. Anti-Spy programs look for signatures or traces that are specific to certain spy software. Some simply do text string scanning to find them, and others actually extract and attempt to remove the spyware.
3. System resources: Poorly written spy software will almost always put a drag on system resources. Watch out for poor system resources, running out of memory, lots of hard disk activity or a screen that flickers.

4. Machine access: Watch for people trying to gain access to your machine. Many software programs that are designed for spying require physical access to the target machine.

5. Installation monitors: Currently on the market are software programs that will log every installation that occurs on the computer. It is best to leave these hidden on the system. It is possible to catch the installation of many spies in this way.

6. Anti-virus: Many anti-virus programs can catch prolific spy software because they are often classified as Trojan Horses. Keep anti-virus software up to date and make sure it is running in the background.

7. Personal firewall: In today’s treacherous Internet it is very helpful to also run a personal firewall. Firewalls will alert the user to both inbound and outbound activity. The user can control what is allowed in and out of his system. Watches for suspicious programs he does not recognize trying to send data out of his system.

8. Smart downloading: The user must take care when downloading to avoid sources he cannot trust.

9. Common sense: The user has to be careful about what he installs on his system. By not running e-mail attachments and read the EULA carefully.

10. Spy software. The user can monitor for spy software by installing spy software on his system first! Since spy software can record all keystrokes it can monitor and record the installation of another spy software.

**IV- Spyware Threats**

Internet threats are constantly evolving and developing. Despite experience with computers and the Internet, many consumers are neither aware of spyware intrusion nor knowledgeable of spyware removal tools available to them. Due to this lack of knowledge, they have not taken adequate steps to protect themselves [3].

Remote monitoring and ad-serving software is just the latest demonstration of how the commercial costs of Internet development are covered in clever and
Spyware is annoying and negatively impacts the computing experience. Even worse, there are real and significant threats to corporate and even national security from those who use and abuse spyware [15].

The dangers of spyware are not always known and are almost never obvious. Usually, one knows when he has a virus or worm—they are quite obvious. Spyware silently installs itself on a computer, where it might start to take any number of different and unwanted actions, including [15]:

1) “Phone home” information about an individual, his computer, and his surfing habits are sent to a third party to use to spam user’s computer or push popup ads to his screen.
2) Open a computer to a remote attacker using a Remote Access Trojan (RAT) to remotely control a computer.
3) Capture every keystroke a user types—private or confidential email, passwords, bank account information—and report it back to a thief or blackmailer.
4) Allow a computer to be hijacked and used to attack a third party’s computers in a denial-of-service attack that can cost enterprises millions and expose them to legal liability.
5) Probe a system for vulnerabilities that can enable a hacker to steal files or otherwise exploit a computer system.
6) After removing the spyware, Internet Explorer would not access Web pages.
7) Modify user settings without the user’s consent, such as automatically changing the designated home page on the user’s Web browser.
8) Another disturbing threat posed by spyware goes directly to the ability of terrorists or others to disable computer networks in times of crisis.

V- Spyware Violations

The most significant violations of spyware are [13, 16, 17]:

1) **Removal violation** occurs when there is either no uninstaller provided for the software (spyware) or the uninstaller is nonfunctional. The uninstaller may be poorly coded or could be a buggy uninstaller.
2) **Distribution violation** is indicated by stealth installation or lack of clear evidence of intention. Examples include undisclosed bundled installs (ad-supported components, toolbars), confusing end-user license agreement (some installers display this information in an unnecessarily small scrolling box, making it difficult to review), and drive-by downloads.

3) **Integration violation** refers to the effect that a given spyware candidate has on the stability of a computer system in terms of system performance. This can be in the form of browser-related or system crashes, utilization of processing power, memory consumption, and bandwidth consumption.

4) **Behavior violation** is indicated by an intentional behavioral change in a computer not made known to the user. For example, a spyware program may carry out another task in the background (hidden from the user). The spyware programs may affect the browser—browser hijack, browser redirection, or replacement of text or graphics.

5) **Privacy violation** is indicated by a connection to a remote system without the user’s awareness to transmit/receive usage statistics or personal information. Data miners typically cause this type of violation.

**VI- Classifications of Spyware**

In this paper, spyware applications are classified in terms of their behaviors, performance, and functions.

1) **Classifications of Spyware Applications in terms of Behaviors:**

   The behaviors that spyware applications may exhibit can be classified into two major categories—**conspicuous** and **inconspicuous**. Conspicuous behaviors are clearly evident to the user, for example, pop-up advertisements or the significant slowing of the end-user’s computer. Inconspicuous behaviors include bundling spyware applications with legitimate downloads, or installation them without user consent. There are six most common types of deceptive behavior exhibited by spyware applications and can be divided into these two categories [1, 18-20]:

   Three **conspicuous** behaviors:
   a) Online advertising.
   b) Change in end-user computer settings.
c) Slowing of the end user’s computer/causing crashes.

Three inconspicuous behaviors:

Three inconspicuous behaviors:

d) Installation without user consent/drive-by downloads.

e) Spyware bundled with legitimate download.

f) Inability to uninstall/remove.

Installation without user consent may not initially produce the level of angst created by more visible practices because end users (particularly novices) are unaware of the method in which the spyware application came to reside on their computer. However, when end users realize that spyware was installed they take great offense.

It is interesting to note the three most offensive behaviors—change in settings, installation without user consent, and bundled—can be viewed as cyber trespassing, as they change an aspect of the end-user’s computer without consent. These behaviors likely evoke such a negative reaction because they endanger a user’s fundamental sense of perceived control. Thus, a simple change by the software maker requesting the user’s permission to change settings, or install their software, would likely result in a much more favorable reaction by the end user.

The least influential of the significant deceptive behaviors was slowing/causing crashes, which denotes frequent error messages and processing speed degradation. This behavior may rank as the least offensive due somewhat to confounding factors. Indeed, computers crash for many reasons, thus end users may not clearly correlate computer crashes as an effect of spyware. For this reason, the slowing/causing crashes behavior is the most difficult to legislate; it is very difficult to isolate spyware as the culprit. However, the behavior is still significant, suggesting that significant productivity losses result from the slowing behavior brought about by spyware.

2) Classifications of Spyware Applications in terms of Performance:

The performance that spyware applications may undertake can be classified into four main categories [6, 16]:

a) The Overt Provider is the category of spyware whereby users consent to its existence and receive positive consequences. Overt providers instigate the considerable prevalence of adware that e-business companies exploit to monitor and analyze user behavior for
business promotion and advertisement purposes. For example, adware is a widespread form of spyware that monitors online activities and triggers advertisements in response to selections.

b) The **Double Agent** is a particularly devious form of spyware. It has the user’s consent, but is damaging to the direct user. These spyware components plant damaging information (such as pornography, performance-hindering settings, or viruses) and then advertise services to the user to manage the problem or remove the offending components, but which then promulgate negative consequences, much like a Trojan. This scenario involves a confounded relationship between user and spyware provider. In this case, the user may not be aware of the spyware installation, which can also be installed a number of discrete ways (for example, bundling with other applications, providing no option to deselect during the installation of another program, or including spyware acceptance in lengthy EULA (End User License Agreement) agreements).

c) The **Covert Supporter** is hidden software that provides positive consequences. For instance, helpdesk personnel have commonly provided support to users by viewing client screens remotely via network monitoring software. Most network middleware allows administrators to monitor and observe network traffic for various productive purposes, including intrusion detection or ensuring adherence to corporate Information Systems use policies. Covert supporters are also commonly designed to monitor user activities, such as the Web sites visited and email, mainly to promote online performance.

d) The **Parasite** is spyware that does not have user consent and promulgates negative consequences. Many users might be surprised that they are under the ongoing remote surveillance of malevolent invaders. Spyware programs are downloaded when visiting certain URLs (Uniform Resource Locator). Such programs can degrade performance and are designed to make removal as difficult as possible. Most user complaints about spyware stem from parasites due to the extent of damage and difficulties associated with their recognition. The parasite is especially troublesome because the user may be exposed to incriminating information (such as pornography) and privacy can be breached without user consent. Significant negative consequences of parasites include both user and organizational concerns. Additionally, parasites affect businesses by stealing user names and passwords to launch attacks, gain access, and impair performance. Attacks may
include downgrading machine performance (in terms of high CPU usage and network bandwidth occupancy), redirecting browsers to spyware-affiliated addresses, and displaying pop-up advertisements that plague user screens.

3) Classifications of Spyware Applications in terms of Functions:

The spyware applications can be classified, in terms of their functions, into eight main categories [1, 4, 10, 13, 16, 17, 21-24]:

a) Adware

Adware displays advertisements while the browser is running. It may track personal information (via data miners) as well as gather information anonymously or in aggregate. Many times adware can be rather harmless, just modifying the ads after the user profile without any kind of automatic information gathering or transfer. However, due to the publicity of spyware lately, adware has gotten a very bad reputation in the eyes of the general public and many companies are reluctant to utilize adware from fear of smearing their company image.

b) Browser Hijackers (or changers)

A simple form of browser hijackers, that "enter user’s computer" when a user visits a web site and for example click an OK-button, attempt to overtake certain functionality of the default browser on a user’s system. One common approach is to change the start page of the browser to one where advertisement is shown. It is also common that the hijacker generates pop-up windows with additional advertisements, sometimes so many that the user is not able to close them all and the browser (or even the computer itself) slows down and crashes.

A more serious form of hijacker that could be distributed together with a normal program installs a BHO (browser helper object) or similar that alters the behavior of the browser. With a BHO it is possible to monitor all the user’s activities within the browser software, such as all typed or clicked URLs and produce arbitrary responses to these events. One consequence of this is that a user’s search strings could be recorded and passed on to a third party.
c) Cookies and Web Bugs

Cookies and e-mail tracking are (or at least can be) a passive form of spyware. They do not contain any code of their own but rather rely on existing Web browser or e-mail client functions. For this reason they are often considered to be a mild form of spyware. Cookies are small pieces of state stored on individual clients’ Web browsers on behalf of Web servers. Cookies can only be retrieved by the Web site that initially stored them.

Web bugs – invisible images embedded on pages – are related to cookies in that advertisement networks often contract with Web sites to place such bugs on their pages.

d) Keyloggers

Keyloggers were originally designed to record all keystrokes of users in order to find passwords, credit card numbers, and other sensitive information. Keyloggers have expanded in scope, capturing logs of Websites visited, instant messaging sessions, windows opened, and programs executed.

e) Malware

Malware (from malicious software) is any type of programming intended to cause harm. Viruses, worms, spyware, and Trojan horses are the most common examples of malware. Among other things, a malware infection can: corrupt files, alter or delete data, distribute confidential data, disable hardware, deny legitimate user access, and cause a hard drive to crash. Frequently, malware is also designed to send itself from user's e-mail account to all the friends and colleagues in his address book. The results of malware infection include wasted resources, compromised systems, lack of regulatory compliance, lost or stolen data, and the loss of user and client confidence.

f) Spybots

Spybots are maybe what most people think of when spyware is mentioned. They closely monitor different aspects of user behavior and transmit the data to a third party. Spybots are different from a normal key logger in the sense that it contains some sort of reasoning about what to collect. This could be the characters typed into secret fields of a Web form, address book entries, a list of visited URLs or any other data found on the host computer. A spybot could be installed as some form of helper object to existing applications or as an application of its own that is launched as the operating system boots.
g) Bundleware

Bundleware (software included with other software) may be installed via drive-by download in which it tries to install from an unrelated Web page, often triggered by third-party advertisements. Bundleware can be installed when users click “Yes” for download, believing it is needed to load the Web page. Aggressive drive-by download uses coercion tactics to try to get the user to click “Yes,” such as by repeatedly opening error windows when the user refuses to allow downloads.

h) Dialers

Dialers change dial-up settings on a computer to connect to another location, which may result in expensive long-distance charges. A stealth dialer makes its calls without any prompting from the user. A hijacking dialer changes the default Internet dial-up connection; so that all future Internet connections are routed through numbers that incur expensive charges.

VII- Well-Known Examples of Spyware [1, 11, 21, 25-27]:

The followings are some well-known examples of spyware:

1) Gator is adware that collects and transmits information about a user’s Web activity. Its goal is to gather demographic information and generate a profile of the user’s interests for targeted advertisements. Gator also tracks the sites that a user visits, so that it can display its targeted ads at the moment that specific words appear on the user’s screen. Gator is also known as OfferCompanion, Trickler, or GAIN.

2) Cydoor displays targeted pop-up advertisements whose contents are dictated by the user’s browsing history. When a user is connected to the Internet, the Cydoor client prefetches advertisements from the Cydoor servers. These advertisements are displayed whenever the user runs an application that contains Cydoor, whether the user is online or offline. In addition, Cydoor collects information about certain Web sites that a user visits and periodically uploads this data to its central servers.

3) SaveNow monitors the Web browsing habits of a user and triggers the display of advertisements when the user appears to be shopping for certain products. While SaveNow does not appear to transmit information about the user’s behavior, it does use
collected information to target its advertisements. SaveNow will periodically contact external servers in order to update its cached advertisements and its triggers.

4) eZula attaches itself to a client’s Web browser and modifies incoming HTML (Hyper Text Markup Language) to create links to advertisers from specific keywords. When a client is infected with eZula, these artificial links are displayed and highlighted within rendered HTML.

5) Kazaa is a peer-to-peer file sharing application. It allows the user to download audio, video, images, documents and software files. The official client can be downloaded free of charge and is financed by attached adware and spyware.

6) RealPlayer includes spyware. It discloses this information in its terms and conditions when installed, though most users don't read the terms and conditions when they install software, particularly if it is free.

VIII- Anti-Spyware

To rid a computer of spyware, then an anti-spyware system is the most widely recommended solution, which implements features that prevent, detect, and remedy the problems caused by spyware. The system monitors spyware attacks and automatically identifies and cleanses a system [28].

Thus far, the anti-spyware model has followed the existing mature anti-virus model: A third-party clearinghouse aggregates the experience, knowledge, and findings of thousands of users, investigates reports of new malicious software, and maintains an often updated anti-malware scanning tool that can be used to examine any suspecting user’s system for traces of known malware [29].

Moreover, cleaning spyware from infected systems is not any easier than ridding computers of viruses. In many ways, spyware intrusion is more difficult to defend against and disinfection is more complicated than viruses. Most anti-virus software packages now prevalent on corporate computers cannot detect the existence of spyware and many spyware programs have a feature that will automatically reinstall if removed. It takes a special breed of anti-spyware software to do the job properly [2].

Several findings pointed out that any single antispyware system could not successfully identify and clean all types of spyware. Therefore, anti-spyware system
experts recommend using multiple systems. This is not desirable since this requires the adopters to expend more effort in maintaining multiple systems, not to mention increased cost [28, 30].

It is also recommended that anti-spyware system developers include explanations that emphasize moral image and innovativeness of adopters in their marketing strategy. For instance, advertisements could explain how an individual’s adoption of an anti-spyware system contributes to the improvement of Internet security. Ads could also emphasize that users of anti-spyware systems indicate savvy computer users and industry leaders [28, 30].

The following are some guidelines to minimize spyware infections [13, 21]:
1) Enforcing the usage of high security settings in Internet Explorer that can override the default security settings or user-defined settings. This can be used to prevent and track sites that repeatedly cause spyware infection.
2) Using Web site blockers and Internet filters whenever possible, particularly on computers used by many people such as those in computer labs.
3) Controlling and monitoring downloads from Web sites because many of these downloads are automatic.
4) Spam controls (for example, SpamJam in the Lotus Notes email client) should be enforced more stringently to prevent incoming email that can initiate spyware dissemination (via hyperlinks in the email).
5) Employing alternate browsers such as Mozilla Firefox, which have built-in pop-up blockers and download managers, can be an effective measure.
6) A firewall is a strong defense mechanism against spyware. If used effectively, it can block spyware from sending information over the Internet and block the self-update features of spyware.
7) Providing real-time protection against spyware with active updates is an effective measure against spyware although it occasionally interferes with legal pop-ups.
8) One way to prevent unwanted or dangerous Internet traffic is to implement some form of “filtering” on the Internet traffic coming into the network. Filtering can be done by implementing a proxy server.
9) Another way of controlling unwanted program installation such as instant messenger software is to configure the network user accounts in Windows to prevent them from installing software unless they are a member of the Windows Administrators group (user permissions). The Information Technology personnel could then control exactly what is installed on network computers.

10) The author of this paper suggests that the operating system must include a mechanism that informs the user about his computer activities (just before shut down), each time he runs his computer. So that the user can check if there are “strange” activities occurred. This can be done by displaying a list of 'tracks' usually generated by the operating system. A “track” is a generic name for information recorded by an operating system or application about actions the user has performed. Examples of tracks include recently visited Website lists maintained by most browsers and lists of recently opened files and programs maintained by most operating systems.

To win the battle against spyware, the following lines of defense should be considered [2, 15]:

1) The first line of defense is **Education** and **Protection**.

2) The second line of defense is **Awareness** which is a key predictor of taking actions. It is clear that the awareness factor emerged as the most significant determinant of user behavior of taking active measures to protect against spyware intrusion and clean spyware from infected systems.

3) The third line of defense is **Disclosure Legislation**. All applications, including those bundled and downloaded along with free software and with legitimate commercial applications, should be readily identifiable by users prior to installation and made easy to remove or uninstall.

4) The fourth line of defense is **Aggressive Prosecution**. The deceptive practices employed by many spyware developers are already illegal under existing laws against consumer fraud and identity theft. Law enforcement agencies at the federal and state level should be encouraged to aggressively pursue and prosecute those who use spyware to disrupt service, steal data, or engage in other illegal activity.

5) The final line of defense is **Planning**.
Spyware is intrusive, annoying, and exploitive software that infects millions of computers worldwide for the benefits and interests of the publishers.

Spyware refers to a category of programs that illegally monitor user’s computer activity, often capturing and transmitting his personal information without his knowledge. In the process, they often cause infected computer to become slow and unstable, and cause problems when it is connected to the Internet.

Spyware will always be running “in the background” performing any unknown purpose of its author’s design. What it may do, who produced it, where it came from, how it crawled into the system, are all anyone’s guess. Keystroke loggers and other programs embedded with spyware can be used to steal critical data. Literally thousands of spyware applications are downloaded every day in large organizations whose employees use the Internet. The probability is high that at least some of those applications are designed to steal passwords and other critical data. Theft through spyware could be the most important and least understood spying tactic in use today.

Spyware is a growing concern across our digital society. It affects computer functions and can pose security risks, including collection and transmittal of information to third parties. As a result, there is a growing body of legislation aimed at combating spyware. However, lawmakers are finding it difficult to build effective legislation because of a universal lack of clearly defined deceptive behaviors exhibited by spyware applications.

Only a combination of education and protection, awareness, disclosure through legislation, active prosecution, and planning will provide the answer needed to address the spyware threat. None of these solutions by themselves is enough.
**X- References**


[12] www.spywareguide.com


[16] www.doxdesk.com/parasite/

[17] www.lavasoft.com
[22] www.safer-networking.org
[23] www.spywareinfo.com
[24] searchsmb.techtarget.com
[26] en.wikipedia.org
[27] www.internet-guide.co.uk