Spyware

Tracking of Information, Counteraction, and Legal Implications

Department of Computer Science
The University of Auckland
June 2002

Michael Chun Long Yip
myip005@ec.auckland.ac.nz

Abstract – Spyware is a type of program which allows companies to track information about users for the company's own benefit. The problem with spyware is that there is no limit to what information can be extracted, and what can be done with it. There are many varieties of spyware, but it generally exists in advertisements and freeware. Spyware betrays the users' privacy and is a nuisance because it adds excessive traffic. Network and software security problems such as the opening of back doors could be added unnecessarily. Many users do not know what information is being gathered; yet they use commercially available software to intercept spyware. Spyware can be harmless if applied within legal bounds, but since companies utilising spyware can use it to their advantage, it may be very easy for them to abuse such powerful knowledge.

Key Index Terms – spyware, adware, FBI, web bug, security, privacy, advertisements, hack, personal information, data gathering, information gathering, logging, GUID, spying, EULA, End User Licence Agreement, Law.

I. Introduction

Fears of "Big Brother" became a big topic in the '90s. The same idea applied to software and computer networks has also brought on just about the same amount of publicity. Only now it is called spyware and consumer misinterpretation and the ease of spreading opinionated ideas on the Internet has created some misunderstandings about

the reality of what spyware is. Most people are familiar with only one example of spyware, but there are a variety of other types of software that are also rightly termed spyware.

This paper will cover definitions of different forms of software that can be labelled as spyware, why spyware is a threat, and what can be done about it. Spyware is a subject with many legal issues. Gator.com sued the Interactive Advertising Bureau (IAB) last year for IAB's "unfounded accusations and threats". One of the most popularly identified forms of spyware is adware, which is free software sponsored by advertisements from advertising companies. The idea is that advertising can lower the cost of software, even to the point of being free of charge. But adware could also have tracking functionality to personally customise effective advertisements for individual users. It is this tracking of personal information that has caused distrust among many users towards advertising companies.

People's opinion of the adware form of spyware is generally negative, even though it originally had positive intentions to allow software developers make money while consumers get free software at the same time. But adware is not the only type of software that can potentially track user information. Commercial software is available for people to intentionally track other people's actions on PCs. Web bugs can be embedded in documents; the FBI uses spyware for their investigations; and some commercially available applications are also known to secretly track user information.

II. DEFINITIONS

Steve Gibson of the Gibson Research Corporation defines spyware as follows [1]:

> "Silent background use of an Internet 'backchannel' connection MUST BE PRECEDED by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed, consent for such use.
>
> ANY SOFTWARE communicating across the Internet absent these elements is guilty of information theft and is properly and rightfully termed: Spyware."
>
> *http://grc.com/oo/cbc.htm*

The “backchannel” mentioned above does not necessarily have to be the Internet. It can also be a private network connection within a company, or it could be non-existent, with the information being gathered stored locally. The form of communication used depends on the type of spyware being defined. In the definition above, the type of spyware being mentioned is of the adware variety. I suggest a simpler and more general definition of spyware:

“Any form of software that secretly gathers information about target users”.

Being secret implies that the target user has no knowledge that the software is gathering personal information. Without the target user’s knowledge of it, the software is doing this without user consent. The target user is not the user of the spyware, but the user of the system or application in which the spyware resides. The user of the spyware is the one who is using it to monitor others. Spyware can come in any form of software, be it an extension, add-on, or specialised application.

Note that spyware is actually different from Trojan horses [2], even though they appear to be similar. The main difference is that spyware does not deliberately open backdoors for hackers to enter. Spyware can be a tool for hackers, and examples of how it could be a security threat will be discussed later in detail.

Because there is such a variety of spyware, it will be useful to clarify definitions here before we move on to what they are capable of. I will classify them into two groups: deliberately installed spyware, and secret/hidden spyware.

The deliberately installed spyware can either be part of another software package, or it may be a software package itself. Adware is of the former kind, which usually consists of two parts: the core software, and the advertising software (see figure 1). The term adware is actually a registered trademark of www.adware.com, but it is in such general circulation that I cannot avoid using it here. Adware can be thought of as the software equivalent of local radio and television broadcasting [3]. Advertising is what makes local radio and television programs free. But the difference is that radio and television programs are not capable of tracking any form of user information. The word adware will be used in the rest of this paper to refer to software that contains advertising, but which may or may not contain spying capabilities.

The opinion that adware is malignant is not unanimous. "Shareware, adware, spyware" [4] claims that there is not enough substantial evidence of adware companies that track user information without user consent. The fact is that adware companies usually do publicly admit that they track user response to certain advertisements, but the companies claim that it is only to target the best advertisements for each individual user. The real fear that people have here is not in what they know is being tracked, but in what they do not know. Just because companies tell you that they track one set of information, it does not necessarily mean that they will not track a different set.

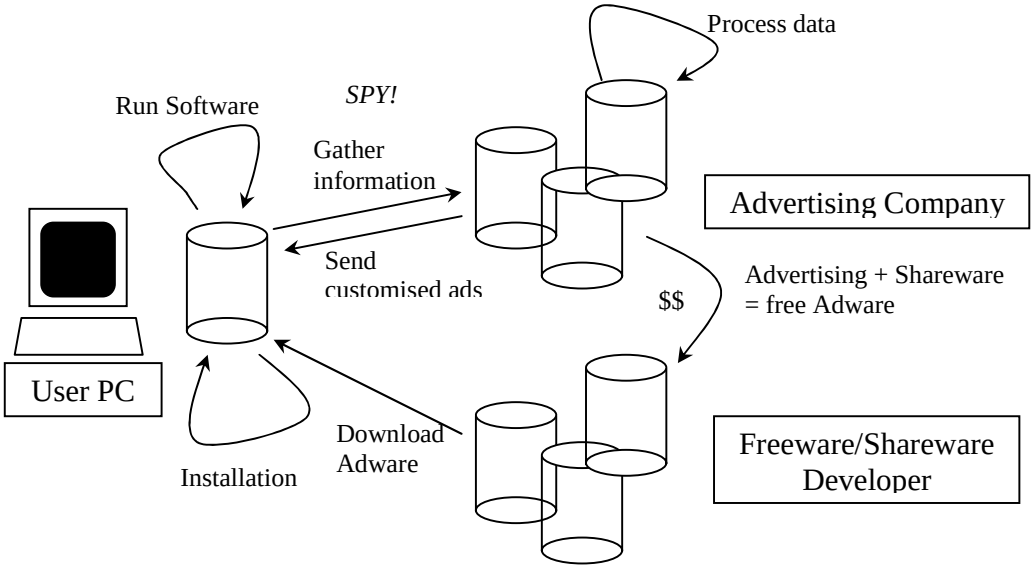

Figure 1. How Adware Works. Freeware is free software, while shareware is freely distributed software that is crippled in some way, by means of time limits or functionality.

Users who intentionally want to track other users' actions can also deliberately install spyware. It is distributed as an independent application and is used for the sole purpose of tracking user information. It does not use other software to hide it, and it runs in the background watching the PC user's every move. SpectorSoft provides spyware for families to monitor the computer usage and actions in the home. It can also be used to monitor employees and students to ensure they are not performing tasks irrelevant to their work. The FBI has used spyware for investigating criminal offences and for producing evidence needed for these convictions. "Keylogger" [5], "Magic Lantern" [5], and

"Carnivore"[6] are tracking software that has been used by the FBI. Keylogger is older software that has to be manually installed in a suspect's computer to track all keyboard inputs. Magic Lantern is a virus-like application that can install itself over the Internet and relay information back to the FBI headquarters. Carnivore has been developed since 1996, and is installed at the Internet Service Provider, with their cooperation, to monitor Internet traffic. The following diagram shows all three applications in the same system.

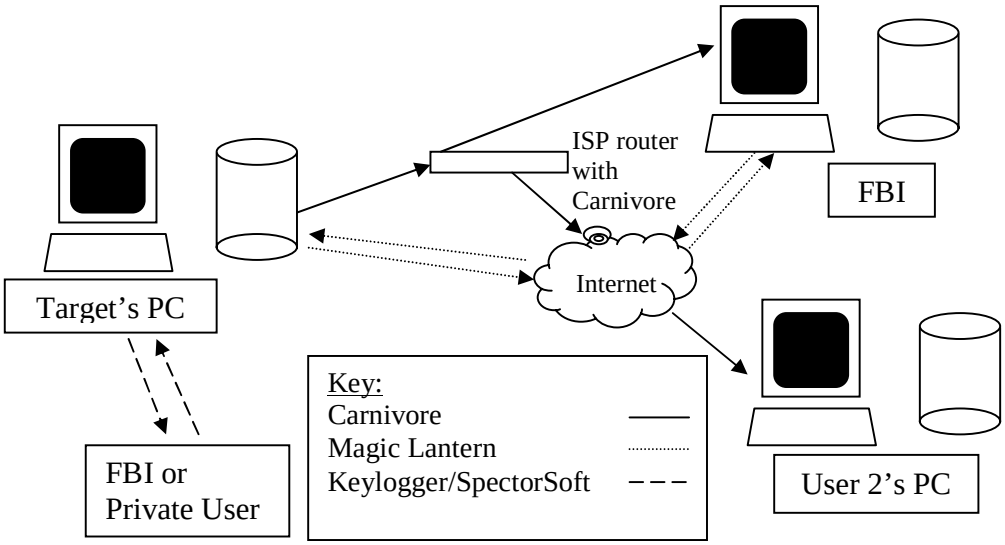

Figure 2. Combined diagram of Carnivore, Magic Lantern, and Keylogger. SpectorSoft provides an application, which behaves in much the same way as Keylogger, but is sold to private users instead.

Hidden spyware is software that has no intention on letting the user know that they are tracking information. The tracking functionality is embedded in the software by the software developers themselves rather than by a separate advertising company. Such examples can be found in commercially available products in which the user has already paid for the software. But the developers, for some reason, decide to stray from its advertised functionality and track user actions within their program.

Web bugs [7] are 1x1 pixel images that can be hidden in web pages, word documents, and even e-mail. It can use be linked to code such as java-script to gather system information such as the user's browser type, operating system, IP address, previously visited webpage, and even cookie information.

The use of spyware can be commercial or private. Adware in particular is commercially oriented. Its main purpose is to help shareware developers make money. It can lower the cost of software, and users could get software for free. Having free software means that more and more people use the software, and thus increases the user base for the adware company. The whole idea is to benefit everyone involved.

Privately, spyware can be used in homes for parents concerned about their children's activity on the Internet [8]. Spouses could even use spyware to spy on their partners if they suspect their partners of infidelity. Corporations and businesses could use spyware to monitor employees, so as to make sure that they are doing what they are supposed to. Educational institutions can use spyware to track students, making sure that they are not using the facilities for non-academic work. The FBI has used spyware [5] to investigate a case where the files needed to convict the suspect were encrypted. "Keylogger" was used to obtain the password necessary to decrypt these files.

III. Information Tracking

What kind of information is collectible through the use of spyware? Spyware can track activities such as browsing habits, screenshots, mouse clicks, and keystrokes. Tracing keystrokes can lead to the discovery of e-mail messages, chat room messages, instant messages, and even browsed web addresses [9]. Information about activities is dynamic and needs to be monitored constantly, but static information such as IP addresses, browser type, and operating system can be retrieved immediately without any extra time used for monitoring.

In order to identify gathered information (from adware) with a particular user, a Globally Unique ID must be used (GUID). This may be constructed from hardware information, username, and software install version. The user's real name may not be known, but this is unimportant for advertising purposes. This GUID may be stored in a cookie, or it may be hidden in the system registry. When data is being sent back to the company, the GUID is also sent with it so that it can be identified with a particular user profile.

If users register their products, then this GUID could be used to identify users to real names and addresses. The same could also happen if the software requires certain

information about the user in dialogue responses during the installation procedure, though in this case, users sometimes do not provide real information since it is generally assumed that such information will not need to be used by the software provider.

The Privacy Foundation [10] tested a set of products suspected of containing spyware, and found that "100% of the tested products had significant problems disclosing their behavior to end users; more than 50% of the products employed data flow that appears to weaken end users' privacy, even though the product functionality marketed to users did not require it".

Users do not know what other information can be gathered by adware. They cannot easily find out by mere packet sniffing since the software developers could easily use some form of encryption to encrypt the data being sent. In order to find out what is actually being sent, users will need to be able to break this encryption. General users have no way of verifying if the data being sent is valid (complying with the user agreement) if they cannot decrypt the data. But should the data be encrypted? If companies stand by what they say, they should have no problem exposing the truth. But then again, if the data is not encrypted, it can be read by virtually anyone on the Internet while it is being sent. So adware companies have a good reason to encrypt the data.

Key logging has the potential of disclosing private information such as passwords, social security numbers, and credit numbers. Users may record personal information such as diaries and journals, and retrieving this type of information is generally accepted as unethical. On the other hand, "Shareware, adware, spyware" [4] unsympathetically suggests that users may be afraid of spyware because they may have questionable content in their PCs.

Not knowing which pieces of information are being tracked is one thing, but there is also a threat in not knowing what may be done with the information. Most users are fine with letting advertising companies know which products they like. But they may object if advertisers use this knowledge to target only more expensive products.

According to Steven Gibson, "Aureate software has been conclusively found to be directly responsible for significant Windows system and Internet browser crashes" [1]. This is a serious security issue as it can open opportunities for hackers to attack. Badly coded adware can make buffer overflow hacks a real possibility. Although any badly

coded program could create this kind of security threat, adware is actually added to existing software developed by a separate company, so the flawed adware could unnecessarily add problems to otherwise safely written code.

IV. COUNTERACTION

To counter spyware, users can prevent it, remove it, or intercept it. Choices in prevention include deciding not to install any product that may contain spyware. This means that the user has to be well informed about adware products. Users will need to carefully read privacy statements associated with products they want to install [11]. Some software provides users with the choice to not include advertisements in the installation.

Users may remove the advertisements from adware instead. This may be done either manually or automatically. To manually remove spyware, merely uninstalling the host application may not help, as the spyware component may be installed separately and could remain installed. The registry may need to be edited (for GUIDs etc…), hidden directories might need to be deleted, and some files could need editing. The article "Rendering Spyware Mute" [12] recommends changing the file containing the host address to contain the loop back IP address (127.0.0.0) instead. For automatic removal, there are a lot of applications available for removing spyware components in adware products (such as Adaware from Lavasoft, listed in the appendix). But the problem with removing the spyware component (manually and automatically) is that it could also disable the useful host application.

Anti-spyware and Anti-virus programs would not be useful since spyware can apparently mutate [13]. Though there is no real evidence of that. Also, Symantec [2] will not include an anti-spyware in their products because spyware is still legal.

Because removing spyware can be very difficult, another viable option for the user is to install a firewall to intercept outgoing traffic. That way, even if the information is collected, it cannot be transmitted and thus will be useless to the spyware company, preserving user privacy. This precaution works with all forms of spyware except ones used for domestic purposes, which could easily be detected and uninstalled if target users have any reason to suspect that they are being watched.

Another simple method of interception is word substitution [6], such as using "banana" for the word "bomb". This can be used to fool the FBI because the FBI uses methods for identifying keywords to sort out the overwhelmingly huge amount of information that can be gathered. The FBI could not possibly process all the available information that they are able to collect.

V. Legal Implications

Through copyright, the modification of software is illegal, especially when software developers explicitly forbid it. Thus, by the nature of spyware removal methods in existence, an attempt to remove spyware could also be illegal.

Current laws (U.S.) are more lenient to spyware than to users. The Digital Millennium Copyright Act, and the Uniform Computer Information Transactions Act has allowed software developers to legally include spyware in their products to protect their intellectual property rights [14]. The Spyware Control and Privacy Protection Act of 2000 [10] only requires that adware companies make their legal statements clear, and allow users the choice of whether or not to install. Failing to do so will result in prosecution as unfair or deceptive acts under the Federal Trade Commission Act. This point of view contrasts with source [14]'s opinion that "the FTC's recent endorsement in its report to Congress of vendor 'self regulation' for online profiling doesn't bode well, because it appears to take an opt-out approach where customers must read all the privacy legalese on sites".

The problem with Privacy Statements and End User Licence Agreements is that they are extremely long. The licence agreement that is meant to be read before installation for eZula's TopText iLookup is approximately 6,000 words long. How many users will bother reading that in one go? And considering that these products may well be installed for evaluation purposes only, it is a very unreasonable requirement for the user.

Not only are Licence Agreements notoriously long, they can contain a lot of legal jargon, and be ambiguous and hard to read. This makes it easy for software vendors to embed clauses about their information tracking so that it can be easy for readers to miss. Software developers often also reserve the right to modify their Licence Agreements and

Privacy statements without notice. Gator.com has all the Privacy Statements and End User Licence Agreements for each of its product versions on its website. It appears that they have stated right from version 1.7 what information is required and what is not necessary. This may sound impressive, but just by looking at the current version; there is no way of telling whether or not they have previously reviewed their statements and agreements.

VI. Discussion & Conclusions

The general usage of the term spyware is in substitution of the word adware. It could be that entrepreneurs targeted advertising companies by creating the notion of spyware to make money off paranoid users, though this is just a speculation. Aside from all this excitement over software laden with advertising, genuinely intrusive spyware exist in different forms. It is this form of known, deliberate use of spyware that proves to be most interesting.

By U.S. law, all these examples of spyware are legal. But the main point people have in objection to such software is that it is unethical. Ethics in itself is another topic. But generally, most ethical ideals are universally accepted, especially in such a rapidly shrinking world. Including monitoring to improve advertisements and reduce prices in adware programs is generally acceptable, as long as the code does not do anything else unexpected. But what if expensive software, that does not require advertising support, contains monitoring functionality also? Microsoft Word and RealJukeBox are just two applications, which have been suspected of unnecessarily tracking user information and actions. In my opinion, such examples are very unethical and uncalled for. As for FBI keyboard tracing and private use, the moral consequences can get quite complicated and both sides of the story (the victims and the spies) have a lot to argue for.

Users themselves have to decide whether installing spyware applications is a good idea or not. In the case of deliberately using spyware to track another user's actions, the decision depends greatly on who is being involved and how serious their motive is. But as for adware, there is no easy way of finding out what information is being passed. There is no reason why gathered data from users could be disguised by the use of

encryption. Therefore the user's choice will come down to how comfortable they are with the information that can potentially be sent through spyware.

Security issues in spyware cover three of the four types of system security threats as defined by Charles P. Pfleeger [15]: Interception, Interruption, and Modification. Users could hack the functionality of adware, or any other form of spyware that uses the Internet, by using a firewall to intercept the sensitive data. Interruption attacks could occur due to system crashes from badly coded adware, and users could also hack adware to modify it so that it cannot function properly. The threats to privacy and security go both ways when users start to turn against spyware.

There are many reasons to be cautious of spyware, but instances of people being gravely affected by spyware are rare. In fact, in the course of this research, I have not found any notion or evidence of innocent individuals experiencing the potentially adverse effects of spyware.

REFERENCES

[1] Gibbs, Mark (2001, May 14). Spying on the Flip Side. *Network World, volume 18 (Issue 20), p38, 1 page*

[2] Post, André (no date). *The Dangers of Spyware*. Retrieved April 5, 2002, from http://securityresponse.symantec.com/avcenter/reference/danger.of.spyware.pdf, *9 pages*

[3] Wang, Wallace (2000, October). Dealing with Spyware. *Boardwatch, volume 14 (issue 10), p192, 2 pages*

[4] Stevens, Al (2000, October). Shareware, Adware, Spyware. *Dr. Dobb's Journal, volume 25 (issue 10), p123, 5 pages*

[5] Matthews, William (2002, March 11). FBI Spyware Avoids Scrutiny. *Federal Computer Week, volume 16 (issue 6), p34, 1 page*

[6] Hogan, Kevin (2001, December). Will Spyware Work?. *Technology Review, volume 104 (issue 10), pp43, 5 pages*

[7] Ryan, Dan J (2000, August 7). Warding Off PC Spies. *Federal Computer Week, volume 14 (issue 27), p46, 1 page*

[8] Fowler, Doug (2002, January 24). SpectorSoft: Cheating Spouses, Porn-surfing Kids and Time Wasting Employees – Beware!. *M2 Presswire, M2 Communications Ltd,* Coventry

[9] Bass, Steve (2001, October). A Counterespionage Guide to Spyware. *PC World, volume 19 (issue 10), p57, 1 page*

[10] Martin Jr, David M; Smith, Richard M; Brittain, Michael; Fetch Ivan; Wu, Hailin (2000, December 6). The Privacy Practices of Web Browser Extensions. *Communications of the ACM, Privacy Foundation, 61 pages*

[11] Plains, Morris (2001, April). Stopping Unwanted Intrusions. *Scientific Computing & Instrumentation, volume 18 (issue 5), p12, 2 pages*

[12] Gibbs, Mark (2001, May 28). Rendering Spyware Mute. Network World, *volume 18 (Issue 22), p48, 1 page*

[13] Savage, Marcia (2001, December 3). Start-up Hunts Down Spyware. CRN, *(Issue 974), p8, 1 page*

[14] Foster, Ed (2000, August 14). Troubled by the Threat of Spyware? Here are Some Tools to fight against it. *InfoWorld, volume 22 (issue 33), p101, 1 page*

[15] Pfleeger, Charles P (1997). Security in Computing – Second Edition. Prentice Hall PTR. Chapter 1 page 4.

APPENDIX

Some Anti-Spyware websites

- http://www.adcop.org/smallfish
- http://cexx.org/adware.htm
- http://grc.com/oo/spyware.htm
- http://www.lavasoftusa.com/
- http://www.spychecker.com