Symantec Security Response

WHITE PAPER

The Dangers of Spyware

by André Post

Symantec Security Response

INSIDE

Contents

Abstract

Spyware programs are applications that send information via the Internet to the creator of the spyware, or the publisher. Spyware usually consists of core functionality and functionality for information gathering. The core functionality appeals to users and entices them to install and use the spyware. The End User License Agreement (EULA) informs users of the information-gathering actions, but most users overlook this information. Information that is sent to the publisher is normally used for improved direct marketing purposes. The type of sent information differs depending on the spyware program. In order for the publisher to properly digest the gathered data, some spyware programs send a unique identifier with the gathered information.

Users often overlook the information-gathering functionaility of spyware, leaving them unaware that the spyware publisher is gathering data from their computers.

About spyware

In this paper, spyware programs are defined as applications that send information via the Internet to the publishers for marketing purposes without obvious notification to users. In this paper, spyware does not refer to Backdoor Trojan Horses that allow hackers to secretly gain information from the computer. The type of gathered information differs depending on the spyware. Some spyware sends only system-specific information; other spyware sends personal information including browsing habits.

Most spyware programs are free programs that are available on the Internet, and in some cases are useful tools. Some examples are:

- Download utilities
- Games
- Media players
- Accounting software

Technically, spyware can be considered as two separate pieces of software that are shipped in one package:

1.) The core functionality that is visible and useful to the user

2.) Information-gathering functionality that gathers, maintains, monitors, and sends user and/or computer information in the background

Spyware is generally distributed in one of two ways: the developers of the core functionality license the information-gathering functionality to merge with their product, or they incorporate their own information-gathering software. After the spyware product has been produced, it is marketed.

The question arises as to why users would want to use spyware. Most users, if not all, are unaware of the information-gathering functionality of spyware programs. Spyware is generally freeware, and the information-gathering functionality is not mentioned before users install the software, making it attractive to users.

How spyware is used

When spyware is used, it sends information to the software publisher. The type of information that is sent varies per spyware program. Let's take a closer look at a spyware Internet browser to see how the spyware program operates.

> John just installed a new Internet browser to experience the "enhanced browsing and downloading experience" as the spyware publisher advertised. The registration process includes answering some questions about personal details and demographics such as name, age, gender, nationality, profession, and level of education. After finishing the registration process, John decides to start browsing and downloading some software. The software downloads slightly faster than with his old browser, making him a happy user of the spyware product. During every browsing session, John is shown several advertisements. Some are interesting to him and others are not. Over time, John follows several advertisement hyperlinks. Each time, the browser notifies the spyware publisher. The spyware publisher constructs a profile based on the gathered information so that John is only presented with advertisements that are likely to be in his field of interest.

This example shows that users of spyware may not be aware of the information exchange that occurs in the background between the spyware program and the spyware publisher.

How spyware operates

Depending on the goal of the information-gathering functionality of spyware, the nature of the gathered information varies among spyware programs. Some spyware programs only send the time of use and other statistical data. Other spyware programs that incorporate improved advertising correlate the gathered data. In order to keep the gathered information linked to a specific installation, all the information sent to the spyware publisher needs to be uniquely identified.

The unique identifier must be stored on the user's computer. There are different methods for creating the unique identifier. The two most commonly used methods are generating a Globally Unique IDentifier (GUID) and storing a cookie on the hard disk during the installation of the spyware program. A GUID contains data that is unique to a computer's hardware. A cookie is the technical term for a file that contains data, which a specific program often uses. The data that a cookie contains depends on the program that creates it. In the case of spyware, a cookie could contain uniquely identifiable data such as the user name, computer specifications, and installation version.

Every time the spyware program sends information to the spyware publisher, the unique identifier is sent as well, allowing the spyware publisher to update the customer database. Figure 1 shows how the spyware publisher and the users are connected, and the data that is stored on each side of the connection.

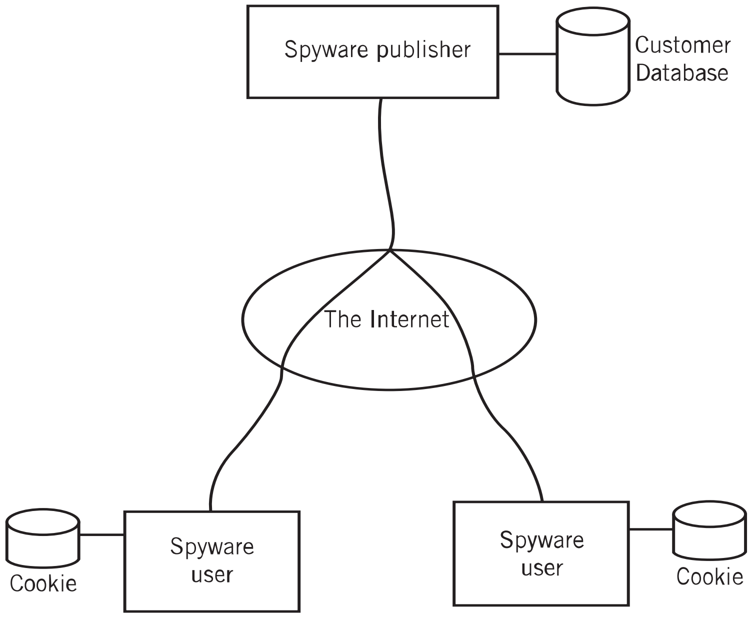


Figure 1: Connections and stored data

User notification

Like most commercial software packages, each spyware program includes a EULA that users agree to before they can use the software. The EULA includes all of the usual clauses, as well as information on the software gathering process for statistical purposes and improved software experience.

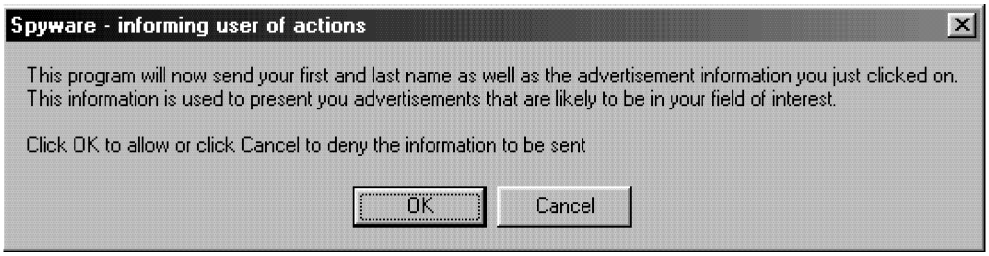
Many spyware EULAs are worded in such a way that:

- They contain so much information that it is difficult to extract meaningful data that deals with the information-gathering functionality.
- The meaningful data that deals with the information-gathering functionality is ambiguous.

This is dangerous because the majority of users accept the EULA without understanding the implications. Many users are upset when they discover that some of the software they use is spyware. They often consider it malicious software. The majority of spyware users remain unaware of the fact that they use spyware. The users in this group may be subject to customer profiling without their knowledge.

At the time of this writing, many requests have been made to spyware publishers to change the EULAs or the products so that users understand what information is sent, when it is sent, and the purposes for which it is used. This can be explained in the EULA in unambiguous, plain language and/or through a dialog box that appears every time the product gathers and sends information (see Figure 2).

Figure 2: A dialog box notification example



Spyware - informing user of actions

This program will now send your first and last name as well as the advertisement information you just clicked on.
This information is used to present you advertisements that are likely to be in your field of interest.

Click OK to allow or click Cancel to deny the information to be sent

This might prevent users from getting upset about spyware, and if implemented properly, it could give users some control over the types of gathered information as well.

Another notification method is for software publishers to set up Web sites that describe the information-gathering functionality of their software. At the time of this writing, several spyware publishers operate Web sites, but the information that is presented on the sites is often ambiguous.

Conclusion

Many users are unaware that they are using spyware because of the poor notification on the information-gathering functionality of the software. This subjects users to customer profiling without their knowledge. For this reason, it is important for users to read and understand the EULA and other notification methods before installing software. It is also of equal importance that software publishers provide users with clear and unambiguous notifications of the actions that their software performs.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product Information
In the U.S., call toll-free
800.745.6054

Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers
please visit our Web site.

The information in this document is subject to change without notice and must not be construed as a commitment on the part of Symantec Corporation. Symantec assumes no responsibility for any errors that may appear in this document. Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holders.

Printed in the U.S.A. 06/03 10061874