TECHNICAL NOTE: SPYWARE

JULY 2004

TREND MICRO INCORPORATED
10101 N. DE ANZA BLVD.
CUPERTINO, CA 95014
T 800.228.5651/408.257.1500
F 408.257.2003
WWW.TRENDMICRO.COM

Spyware — a Hidden Threat

Technical Note

TABLE OF CONTENTS

OVERVIEW 3

DEFINITIONS 3

HOW DO SPYWARE PROGRAMS GET INTO YOUR NETWORK? 4

RISKS OF THESE THREATS 5

July 2004
Trend Micro Incorporated

OVERVIEW

Spyware programs are a growing threat to corporations today. Reports now show that nearly one in three computers are infected with a Trojan horse or system monitor planted by spyware.[1] These hidden software programs gather and transmit information about a person or organization via the Internet without their knowledge.

With spyware's rapid proliferation, organizations are in critical need of anti-spyware technology. Although many point solutions claim to do the job, the most effective defense involves a fully integrated security system with antivirus and anti-spyware on a single platform. This empowers IT administrators to more efficiently manage a coordinated defense against all forms of malware—including the growing threat of spyware.

The following technical note defines spyware plus other extended threats and explains how Trend Micro products effectively protect against them.

DEFINITIONS

Spyware

Spyware is software that monitors a user's keyboard activities and transmits this information back without the user's knowledge. This violation of privacy on the Internet is a major cause for public concern. According to an audit by Earthlink, spyware infects an estimated 90% of all Internet-connected computers. Recent spyware attacks have exposed individual users and corporations to identity theft, data corruption, or personal profiling.

In general (and in this paper), the term spyware is used to describe other types of extended threats, including adware, hacking tools, and more. Although these threats share many similarities, they each have their own unique characteristics, which are explained below in detail.

Adware

Adware is a type of Spyware program that transmits a user's personal information to advertisers who then use the data to send targeted ads to the user. Although it is seemingly harmless, it gathers personal information for marketing purposes, including the user's age, sex, location, buying preferences, and surfing habits. In some cases, it even compromises the user's Web surfing experience by hijacking Web pages and displaying other marketing content.

[1] From article: **Spyware Is Everywhere** - By Gregg Keizer, TechWeb News

Dialers

These types of programs permanently change dial-up settings on a computer to connect a modem to a remote location, resulting in expensive long-distance charges and exposure to other spyware programs.

Joke Programs

Joke programs are applications created and distributed for amusement reasons only. In general, these programs are harmless. However, they can be annoying and distracting. Worse case scenario, an offensive joke opened in a corporate environment could lead to a liability lawsuit.

Remote Access Tools

These are tools created to enable remote administration for legitimate purposes. However, due to limited functionality, there is no proper notification or visibility to inform the user that the remote access tools are being installed. This means they can be used for malicious intent to obtain confidential corporate information from a remote system—without being tracked.

Hacking Tools

These are tools commonly used by network administrators to test the weakness of their corporate systems. However, if these tools fall into the wrong hands, they could be used illegally to access confidential corporate systems and steal data.

Password Cracking Applications

IT administrators use these applications to test the weakness of passwords within their organization. However, they can also be used for the malicious purpose to get users' passwords without their knowledge.

Other

There are a variety of other spyware programs that are not as common nor widespread. Nonetheless, they still present a serious threat, and Trend Micro™ anti-spyware technology is designed to detect and clean these spyware-related programs.

HOW DO SPYWARE PROGRAMS GET INTO YOUR NETWORK?

Spyware programs can enter a corporate network when a user downloads legitimate software that includes a spyware-type of program. Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA includes information about the program and its intended use to collect personal data. However, in most cases, users overlook this information or do not understand the confusing legal jargon. Hence, the user expects to only download the legitimate software but unknowingly downloads a spyware program as well. This may happen, for example, when a user downloads P2P or other types of free file sharing applications like KaZaA.

In addition, some spyware is installed as a standalone application. In this case, similar to the first example, the user is often caught unaware because he or she did not read or understand the license agreement. In both scenarios, spyware programs cannot be blocked by a firewall because the user has requested to download the program. Also, the programs cannot be blocked by traditional antivirus software because they are not malicious in nature and don't share the same behavior as viruses. In some cases, the user cannot get rid of the software because some of these programs can reinstall themselves.

RISKS OF THESE THREATS

Spyware and related threats introduce a significant security, confidentiality, and legal risk to the enterprise. As more corporate PCs get infected, the organization will encounter a greater number of problems, such as:

- Loss of confidential personal or corporate information
- Lower computer system performance
- More frequent system- and browser-related crashes
- Loss of network bandwidth
- Increased remote access costs
- Decreased employee productivity
- Higher risk of legal liability

The impact is clear: spyware programs are much more than a nuisance to the end user and corporate IT managers. The invasion of privacy, threat to security, and damage to the network create a very serious and legitimate public concern.