Posted At: Wednesday, February 18, 2004 7:28 PM
Posted To: Microsoft Outlook Embedded Message
Conversation: public comments
Subject: public comments

Before going into my comments, I will provide a brief outline of my background. I am a software engineer with almost 18 years of experience, including 15 years in the telecom industry. I have worked on a variety of things in the area of secure commuting, including systems involved with national identity cards as well as being responsible for the security of a network of computers.

The area that really concerns me with "spyware" is the implications for national security and privacy in systems that are required, by law, to protect privacy. For example, HIPAA [Health Insurance Portability & Accountability Act] went into effect last year, with strong legal sanctions against those who would violate medical privacy.

There are pieces of software available, which are sold commercially, that make a mockery of attempts to protect national security or legally protected private information. For example, my current employer uses software from SpectorSoft Corporation, 333 17th Street, Vero Beach, FL 32960, (888) 598-2788, that is explicitly designed to secretly record every key stroke, screen display, Web site visited, and e-mail from a computer user.

In addition SpectorSoft's programs have a "stealth" mode where the computer user doesn't even know they are being monitored, and the software goes to a great deal of effort to hide it's actions. SpectorSoft's license agreement claims that companies are required to notify users about the monitoring, although companies, including my employer, did not notify anyone that they were being spied on.

Programs such as SpectorSoft's not only record this data on the company's servers, they also send it encrypted across the Internet to outside computers, including to a machine belonging to SpectorSoft. I know this because I detected how their software misused the Windows Explorer component of Microsoft's Windows operating system.

The ability to silently monitor anything typed and anything on a computer user's screen has grave national security implications. There is nothing to prevent someone with access to a PC from installing these kinds of programs, and then sending classified or sensitive information to people who are not friendly to the United States.

As I mentioned before there is nothing to prevent material that is legally required to be private, such as medical records under HIPAA or credit card information, from being sent out to anyone either.

Given the nature of these programs and their high potential for abuse, I believe they should be treated the same way computer viruses are treated. Computer users should be notified that they are being monitored, what is being monitored, and where the information is going to.

Paul McGinnis
CA