From: Judson Rosebush
Posted At: Thursday, April 29, 2004 1:47 PM
Posted To: spywareworkshop2004
Conversation: Spyware Workshop - Comment, P044509
Subject: Spyware Workshop - Comment, P044509

Without having the time to read all on this subject please let me express a simple thought that I do not much see expressed in the press:

The use of spyware on my computer (or computers in my company) constitutes theft. And stealing is a crime. What is stolen are my CPU cycles, and my ability to use the machine for my business's purposes.

Although I understand there is a free speech debate surrounding this issue, that argument is of no concern to me. The right of free speech does not include the right of strangers to intrude into my office and speak to me or to paint slogans on the walls or my screens.

It is a crime for an uninvited person to walk into my office and use my xerox machine, make long distance telephone calls, use my electricity to, consume my food, or look at and memorize my customer address lists. (The same is true for invited person to do this secretly.)

The access method for the theft is irrelevant. In fact, if they hook a machine onto my electricity outside my building but within the parameters of my electric meter they are stealing. If they drill a hole in the wall and pump out my heat, if they tap into my water, siphon off my gas it is still theft. If they dial into my bank and transfer money out of my bank account it is theft.

Our computers are valuable production resources and their efficiency, like that of any other machine, is valuable to us. Our margins are narrow, the people who operate the machines are expensive, the space the machine occupies costs money. A person who sneaks into a factory and uses a punch press to make holes is stealing, even if he punches it out of his own metal. And a person (or corporation) who sneaks into my company and uses my machines, such as my computers, is stealing. What is being stolen is very simple, and that is CPU cycles, the ability for the machine to perform calculation. If the computer is doing the thief's calculation it is not doing mine. Secondary to actual theft of the CPU cycles is the time of the person operating the machine, the capital value of the machine during the period involved, and the support structure place the machine on a desk.

The thief in this case may argue that the amount of theft is inconsequential. This is not true in the singular case and it is especially not true in the class case. The facts are that this practice is affecting millions of computers, and as a class this affects trillions of trillions of CPU cycles, and the corresponding time lost is enormous is measured in the man-centuries. Added to this is the time to detect the thief and chase him out.

Sometimes the "guest" may argue the he has obtained "consent" to engage in the use of the company's resources. This argument fails to stand up to scrutiny. It is one thing if a guest asks me or an employee if they can use our telephone to make a call. It is quite another for them to set up a telemarketing business within our place of business. In order to do the latter properly (and apparently not in an isolated casual way but in a systematic sneaky fashion) it is imperative that the "guest" establish a minimal business relationship which would include issues of access to the premises (being given a set of keys), proper business licenses, landlord/tenent/subtenent issues, compliance with labor laws such as unemployment insurance, consideration of any union rules, general liability and insurance, work for hire issues, and any rules that involve barter and taxes. No employee of this company is empowered to trade, barter or sell company services for personal gain, and to solicit an employee for this purpose is a crime. No such "agreement" made is enforceable. Who ever heard of a situation where an employee could legitimately pass mailing lists in exchange for some baseball tickets, or take bribes for directing advertising to the boss or other employees? Although an employee may be lured into thinking that their best friend can sit in a black bag and harvest the keystrokes of the workers around them, the quid-pro-quo of a business relationship is not so simplistic. In other words, the spyware cannot legitimately harvest my CPU cycles without an attendant business relationship, any more than a Dupont employee can let anyone walk through the door and configure one of their assembly lines to manufacture some chemical.

I am quite sure that other arguments against spyware are also valid: theft of data, theft of bandwidth, and so on; my point here is to stress the value of the basic resource--the computing machine.

I do understand there are times when processes are downloaded and then executed on a client's machine. A normal web page is an example of this, cookies are another, software that is downloaded for the purpose of execution is another still. The difference is largely one of expectations and intent--and the hated pop-up windows are a good example of where these collide. But if I am trying to walk into a Starbucks to buy a cup of coffee, and a person from a competitor pops up in my way it matters little if I have just walked into the door or am about to put my hand on the knob to enter; in either case my trajectory is being obfuscated. If I quit a website and a popup asks me if I really want to leave or offers me another destination that may be acceptable, but if, when I close that popup two more pop up at me that is abuse. Although some may argue that the issue of spyware is one big gray area that is far from the truth. The boundaries are very traditional and they have to do with the normal expectation of the surfer, common sense, and the normal use of resources. If someone wants to use the resources of my computing factory (my design studio in my particular case) they can come through the front door like any other client.