No. 79, Jun 2000

THE COMPUTER CORNER

Privacy and a Personal Firewall

- by Stan Kaplan, WB9RQR
105 Martin Drive
Port Washington, WI 53074-9654
(262) 284-9346
skaplan@mcw.edu

If you are at all attuned to computing issues in the news, you might have noticed that several places have printed articles lately concerning consumer privacy on the Internet. Two examples are BIG BROWSER IS WATCHING YOU (Consumer Reports, May 2000) and KEEPING YOUR PRIVATE INFORMATION PRIVATE (by Brett Glass in PC Magazine, 6Jun2000). It is an issue looming larger and larger with each passing day. I am not talking here about paranoid delusions that nefarious individuals are trying to get information about you. Rather, I am talking about real efforts by companies to "mine" data, including your personal data, for their gain. The scary thing is that this data mining goes on not just daily, but every second of every day. It is done without your permission or consent, and it is done without any indication to you that it is happening. At present, this is a perfectly legal activity in this country, although it is illegal in much of Europe.

Yes, cookies are part of this story, but I won't go into cookies again in this article because I have written about them in the past and the problem goes much deeper than that. For example, Steve Gibson (Gibson Research, Inc.; http://grc.com/optout.html) recently unearthed the fact that a company that puts banner ads on websites collects information on which ads you click and the time you spend reading each one. It sends that information back to the company, without your consent and permission. Even scarier, this information can be associated with YOU, your name, address, telephone number, social security number and anything else about you that has been given to anyone through your computer. Even if you have not sent this critical personal data out to someone from your machine, if it exists on your hard drive, unscrupulous persons, in the background, can access it while you are connected to the Internet. The worst news: not only is your data available for access, it probably has been accessed several or many times. Let me again emphasize that all this is done without your knowledge and with nothing on your screen to alert you. It is a completely covert intrusion.

"Come on, Stan, you really are getting paranoid" is probably what you are thinking at this point. Well, folks, that is exactly what I thought too in the past when I occasionally heard such allegations. But that changed when I began to read on the subject. I urge you to begin, too. At the very least, log in to Steve Gibson's site referenced above, read his stuff, and perhaps download his tiny program (Optout.exe) to do a test of your ports to see how vulnerable you really are. After that, you will want to read further. Then, when you are convinced, come back to this article to get the following address for an essential software package:

http://www.zonelabs.com/zonealarm.htm

ZoneAlarm is a program classed as a personal firewall. In a car, the firewall is the barrier that separates the engine from the passenger compartment. In the computing world, it is a security level between you and the Internet. ZoneAlarm will halt any intrusion into your machine. It will then pop up a menu telling you of it's action, the Internet address of the intruder, and ask you if you want to grant permission or not. Moreover, it will also block any of the software installed on your machine, such as Internet Explorer, Netscape and others that routinely send out data to their "homes" without asking your permission. You can grant permission for each instance of an attempt if you feel the attempt is justified. Alternatively, you can grant blanket permission to a program that routinely needs web access, such as Norton's antiviral software, which needs to access the Internet periodically to update virus definitions. Or, you can deny permission.

Sound interesting? I bet you are wondering how much it will cost. Well, get this. It is free for individual use!!! The only cost is your time, to download (1.6 Mbytes), install and learn how to use it. The user interface is well designed, everything is intuitive, and it is quick and easy to learn how it works and how to use it to your best advantage. Then, you can forget about it. Until it pops up to tell you there has been an attempted intrusion! As mentioned before, it will also supply you with an Internet address of the intruder, but in numerical format like this: **205.183.255.0** If you are curious as to who this is, you can go to a website at **http://www.arin.net/whois/index.html.** There, you can type in the number and the site will show you as much information about the addressee as is found in the ARIN database. ARIN (American Registry for Internet Numbers, Inc.) is the non-profit organization that allocates IP numbers such as those shown above. Every Internet address in the world has an IP number, which computers and routers use directly (converted to binary), much like a house number. The address we humans use is an association of this number with letter strings that our human brain can use much better than strings of zeros and ones.

My best advice to you is to get and install the program immediately and don't be without it in the future. Not just because the program is so neat (which it is) or because it is free (which it is). Rather, because it will take you a light-year jump ahead in personal security. I think that Zone Labs has done the American Computing Public a huge service by providing it free, and I hope the company does very well in it's commercial sales by way of reward. This program is now on my list of absolutely-must-have software. Happy computing!