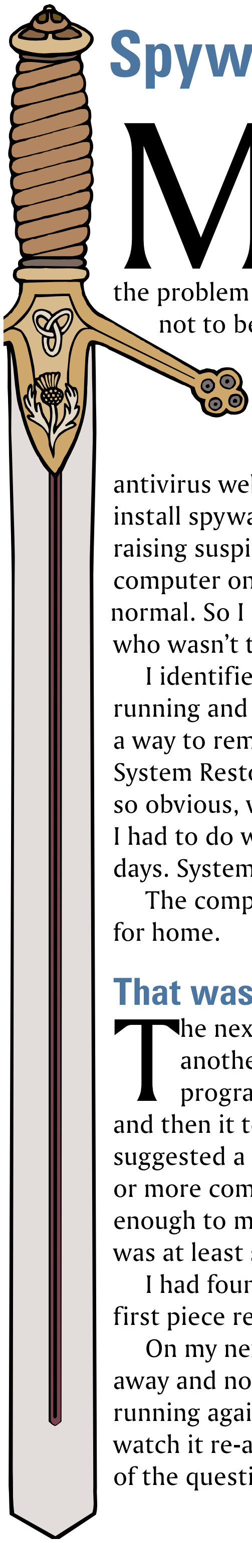
RANDOM THOUGHTS

Communications With A Purpose

William Blinn Communications
179 Caren Avenue
Worthington, Ohio 43085
614-785-9359
Fax 877-870-4892
www.Blinn.com

November 2005



Spyware dangers continue to increase.

My older daughter is careful when she's online, but she called recently with some bad news. "The guy at Roadrunner thinks there's spyware on it." And indeed there was. Finding the problem was easy. Getting rid of it turned out not to be so easy.

Whatever had taken over the computer made sending or receiving e-mail impossible and also eliminated access to all websites – not just to antivirus websites, but to any websites. People who install spyware generally want to do so without raising suspicion because they'll have access to your computer only as long as you think everything is normal. So I knew that I was dealing with somebody who wasn't too bright.

I identified some suspicious processes that were running and eliminated them. As I started looking for a way to remove the infection, it occurred to me that System Restore might help. Because the problem was so obvious, we knew exactly when the it started. All I had to do was move the computer back in time two days. System Restore did that easily.

The computer seemed to be clean and I headed for home.

That wasn't the end of it.

The next day, the antivirus program found another infected file. "But when I tell the program to delete the file, it says that it did and then it tells me the same file is infected." That suggested a *blended threat* – one that involved two or more components. The author who wasn't smart enough to make his program get out of its own way was at least smart to install it in two pieces.

I had found the second piece and removed it. The first piece regenerated the infected files.

On my next trip, I found the infected file right away and noticed that the suspicious services were running again. I could delete the infected file and watch it re-appear. Simple, easy solutions were out of the question.

Finding the problem behind the problem.

The visible part of the problem was "rdriv.sys" in the windows\system32\ directory. This time System Restore wasn't my friend. I shut it off and that caused the deletion of all previous restore points. I didn't know which of those had been infected with the first piece of the malware puzzle, so it was important to jettison all of them.

Next I used MSConfig to disable all services and all startup applications, then rebooted the computer. Running with all processes turned off is similar to running in Safe Mode.

Using the Registry Editor, I searched for instances of of the two infected components – "rdriv" and "wscsvc". This is harder than it sounds because the letters "rdriv" occur in a lot of Registry keys. I needed to be certain that the ones I deleted (after exporting the key to a file, of course) were ones that had something to do with "rdriv.sys". Because the rogue service was dead, I could delete windows\system32\rdriv.sys and it would stay deleted.

Running MSConfig again, I re-enabled all but two of the services and all but two of the items listed in StartUp – the ones I suspected to be the cause of the problem.

Rebooting generated no warning messages, but I ran a full scan anyway: AVG Antivirus found and deleted one infected file. It did not re-appear.

As the scan was running, I used Internet Explorer to visit Microsoft's Windows Update. More that a dozen critical updates were waiting to be installed. The Automatic Update section of the Control Panel revealed that Automatic Updates had been turned off! How? We still don't know.

Where did it come from and what did it want?

Finding the source of the infection wouldn't be easy and probably isn't possible. The two most likely sources are Instant Messenger or a rogue website. Because a lot of security patches were missing, I'm inclined to think it was a rogue website – maybe one that was the result of mis-typing a URL.

I'm not sure what the author's intent was, either. The malware had a "backdoor" component, so it made the computer available for use by somebody else. Given the quality of work evident in the malware, the backdoor component probably didn't work right, either.

At least that's what we're hoping. ß

Random Thoughts (ISSN 1543-1525 [print] – ISSN 1543-1533 [electronic]) is a publication for clients and friends of William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085.

Avoiding spyware isn't easy, but it can be done.

One problem with the Internet is that it's hard to know who's offering you something. A browser add-in that somebody offers you might promise to do something useful – and it may do what it promises to do – but the information you see may not tell you about some of the application's other features.

It may do something relatively harmless such as download advertisements and display them to you. Or it may install a "backdoor" that gives the author access to your computer without your knowledge.

Before I install an ActiveX control, a Java applet, or an application from a company I know nothing about, I do a little research. Using Google to search for the name of the application and the word "spyware" can be helpful, even if it's not definitive.

Additionally, I have a firewall that monitors outbound traffic. Whenever a new application wants access to the Internet, I give it conditional approval to see what it will do.

Beyond being careful with what you install, it's important to install antivirus and anti-spyware applications and to keep them up to date.

Here are some that I recommend.

First, make sure that the Windows Automatic Update feature is turned on and be sure that your antivirus program and firewall application update themselves regularly – once per day isn't too often.

Spyware Doctor is a good anti-spy application from PC Tools (www.PCTools.com). There is no free version available, though. If your budget is a bit on the thin side, combining 3 free applications gives you essentially the same coverage:

- Visit Safer Networking (www.Safer-Networking.org) and download *Spybot Search and Destroy*.
- Visit JavaCool Software (www.JavaCoolSoftware.com) and pick up *SpywareBlaster* and *Spyware Guard*. (Note that "SpywareBlaster.com" is not the home of the program you want.)
- The previous 3 applications are free for use in homes or businesses. For non-commercial use, you may obtain the free version of *AdAware* from www.Adaware.com. Business users must purchase a license.

Browser and instant-message choices.

Windows computers all have Internet Explorer installed, but you may want to consider one or more of the other free browsers. No browser is perfect and all browsers have security problems, but these three are less likely to be targeted than IE is and there are better IM choices than AOL's application:

- *Firefox* browser from www.mozilla.org.
- *Netscape* browser from www.netscape.com.
- *Opera* browser from www.opera.com.
- If you use instant messaging (AOL's or any of the other services), avoid using AOL Instant Messenger. Instead, pick up the free *Gaim* instant messenger tool from SourceForge.net/projects/gaim/. It's much more secure than AIM.

If you're using Windows XP, make sure that service pack 2 has been installed and, if you don't use *Zone Alarm* or some other firewall, that the Windows firewall is enabled.

And still you're not finished.

You are the final part of every security system. You're the one who must ensure that applications are regularly updated. You're the one who must analyze any application before installing it. You're the one who must resist the urge to click a link or open an attachment in any message from someone you don't know. And you're the one who must consider with caution any attachment, even if it seems to be from someone you know.

Malware is almost always obvious to the person who examines things carefully. Spending a few seconds to contemplate an action is far better than spending several hours undoing the effects of a careless action. ß

Open Office 2.0 "ships"

Can a downloadable product *ship*? If the version 1.9 beta code doesn't differ a lot from the version 2.0 code, is it a big deal? Is Microsoft concerned that a "free" office suite is nearly as good as *Microsoft Office*? The answers are no, yes, and yes.

Putting a visit to www.OpenOffice.org on your to-do list might be a good idea. The office suite is a 75MB download. It may be just what you're looking for.

Earlier versions were buggy and slow, but version 2.0 is impressive. It offers advanced XML capabilities and native support for the OASIS Standard OpenDocument format.

Whether *Open Office* is finally good enough for you is something only you can decide. I've used the late beta occasionally over the past few months and have found that it does most of the tasks I need it to do.

Heavy *Powerpoint* users or those who need some of *Word's* heavy-duty advanced features won't be satisfied with *Open Office* and the next version of the Microsoft product will raise the bar a couple of notches beyond where it is now.

But if your needs are modest, the Open Office suite may have finally hit its stride. It is worth taking a look. After all, there's no charge to download it or to use it. ß

on the market CORNER by A.J. Stinnett

"Communication
in an organization
is defined as the
free exchange of information."