Radio Days – 2012-07-14

Tip of the Week – Secunia PSI

I have spoken in the past about keeping your computer, and its programs, up to date. There are various programs and methods of achieving this, but the one that I recommend is Secunia PSI. This free program helps you keep all the programs on your computer up to date.

Since the final version of Secunia PSI was released two weeks ago I have had a chance to see it in action on several computers. In almost all cases this program has worked to update all the programs on all the computers with no intervention. However, there have been two computers where manual intervention was needed.

- In one case there was an old version of Java which should have been removed during an earlier update of Java. This, for some reason, had not happened. After I had removed this old version manually all other updates worked perfectly.
- In the other case there was a downloaded copy of an old version of Firefox sitting in an unused folder. Removing this old program again allowed all the other updates to complete normally.

To find out what the reported problem means is simple: just right-click on the offending program then left-click on the bottom option. I am sorry that I cannot remember what this bottom option is: please take this as a compliment to the effectiveness of this new version of Secunia PSI!

Again, I cannot recommend this program highly enough!

DNSChanger Virus: What, Why, How

This week's talk is about a virus which only stole about $14 million from its victims. It is easy to ensure that you do not get it because it has been around since 2007: that is five years ago! This is more than enough time for the anti-virus writers to have worked out how to stop this virus yet people are still being infected.

You may have heard about it: it was reported on SBS news early this week. This is important because, at 2 pm Victorian time on Monday, the computers which had protected internet users were switched off. At this time there were an estimated 200,000 infected computers in Australia, and these computers would not have been able to access the internet.

Was your computer one of those infected with the DNS Changer virus?

How Does DNS Changer Virus Work?

The reason that this virus was able to steal money from its victims was that their computer was routed to the wrong place on the internet. The way that this virus works is, in essence, very simple. When you type in the address for a web page (eg www.tobybainbridge.com) your computer has to be able to convert that address to the equivalent numeric address which the internet uses. In this example www.tobybainbridge.com is translated to *180.214.68.3*: this translation is needed because people find it easier to use words but their computers only understand numeric addresses.

The computers which translate our words to a computer's numbers are called *DNS servers*. *DNS* stands for *Domain Name System* and these servers have to be trusted absolutely: if there is any error in the DNS servers then the whole fabric of the internet falls down.

If criminals can use their own DNS servers to ensure that you are taken to rogue sites which ask for, and get, login details for your banking details then you will soon be stony broke. This is what had happened to many people: and these people are left wondering what hit them.

The FBI

In the early stages of the DNS Changer virus the FBI noticed what was happening and worked out that the best way to fix the problem *in the short term* was to replace those rogue DNS servers with ones that returned the numeric addresses for the wanted websites. This could only ever be a short-term fix: if left in place for ever then people would not bother to take the precautions needed to keep their computers safe.

The court-approved replacement DNS servers had to be removed on Monday 9 July. This meant that those computers which had been infected with the DNS Changer were then liable to be directed to the rogue websites with the possible loss of money or identity. According to internet sources all those people who were infected with the DNS Changer virus were told to clean their computer or to get some help to clean their computer. Those who did not take the needed action will, by now, probably be unable to get onto the internet.

Does this include you?

The Symptoms of Infection

If you are infected with the DNS Changer virus you may notice that your internet connection does not work or works very slowly. There are many causes for a slow internet connection other than the DNS Changer virus. If you have a slow connection, or if you cannot access the internet at all, you need to determine what the problem is if you want to access the internet. If you are unable or unwilling to do this then my advice is to get professional help.

There are some simple checks which you can do at home to see if the DNS Changer virus is the cause of your slow, or missing, internet connection. The easiest check is to type in the internet address which you want as numbers rather than letters. Here are some numeric addresses for you to try:

www.dns-ok.gov.au	165.191.2.65
www.australia.gov.au	205.239.168.12
www.abc.net.au	203.134.26.42

Type one of the numbers given above into the address bar at the top of your web browser where you normally type the name of the website which you want then press *Enter*. This will display the website which you would expect the see if you have internet access. If you cannot get the website to display then you have a problem which I cannot help you with in this document. You will need to get help from someone who can come to your home or office and check your internet connection and other details.

If you can get onto the first of these websites you will be told whether you are infected with the DNS Changer virus. If you get a green message which states:

You do not appear to be affected by DNSChanger

then you can relax. This means that your computer has either not contracted the virus or that the virus has been removed. Now you know that your anti-virus program is up to date and working well. Congratulations!

If you do not see this message then you will have to take steps to ensure that your computer is cleaned and disinfected. You may be able to take these steps yourself or you may need help. I suspect that, if your computer is infected, you will need help because if you knew enough to keep your computer clean you would have done so.

Please find a good support person who will come to your computer and fix the problem.

Further Information

Secunia PSI	www.secunia.com
DNS Changer Check	www.dns-ok.gov.au