June 2005

Smart Sheet

Technology Information Newsletter of

Smarts On Site
Computer Support Services
705 – 734 - 0597

Computing's enemy No. 1...

by Stephen Bungay, Smarts On Site

Ourselves! I know it's a difficult pill to swallow but it is nonetheless true. The promise of multimedia and on-demand entertainment are the lures used by adware and spyware companies, as well as organized crime, to infect out computers with all kinds of nasty bugs.

Downloading the latest movies (perhaps before they are even out of the theatre) and music from the web is a great way to not only get yourself in big trouble with the law, but also have your personal computer polluted with adware and spyware.

Advertising on the web is a business of pennies, each click on an advertisement or each time an advertisement pops up there is an exchange of a few cents... perhaps less than one. The small amount money changing hands is made up for by the sheer volume of pop-up advertisements being displayed. Think millions per hour!

I once again ran into one of the worst offenders, a small executable file called “nail.exe”. This comes from a service named “A Better Internet”, something I'm sure everyone would like to see brought into existence, and something that many people would click on if they saw the chance to make their Internet experience truly better.

Social engineering at its finest. A Better Internet means just that, but not for you, for the adware and spyware company. They reap the rewards while your business or personal computer slows to a crawl and your browser gets its homepage randomly hijacked to sites advertising their wares, and thats much better isn't it? Smarts On Site

INSIDE...

Could deleting spyware become a criminal act?

By Stephen Bungay, Smarts On Site

In the United States, the passing of a law that makes spyware illegal might just end up protecting those who profit from the stuff. How could this be? Read on.

Some background

It all starts with defining what spyware actually is. Spyware spys on us, it watches our activities on the Internet and reports on what we're up to. Adware on the other-hand, may not fall into the classification of spyware if all it does is display a random series of advertisements. The exception to this would be if the adware displays advertisements which are in context with whatever you are looking at while surfing the web. Spyware is usually installed without your knowlege. Adware sponsored programs, on the other hand, may inform the end-user that the adware is being installed along with the package, and the advertisments can be removed if you buy the program.

Ties that bind

The business model of using sponsors is as old as the business of publishing newspapers and magazines, but there is a difference. Magazines and newspapers do not have an End User License Agreement (EULA). The EULA is the agreement you consent to before most software will install on your computer. When you click on an "accept" or "agree" button you have in essence entered into a contract. Did you read it? If this contract informs you that programs will be placed on your computer to provide advertisements or collect marketing demographic information then the spyware is no longer an illegal product that was covertly installed on your PC.

Breaking up is hard to do

Maintaining the functionality of advertiser supported software after removal of it's adware or spyware could be construed as breaking a contract. If you break the contract then you give up the right to continue to run the software and if you do continue to run the software then you may be opening yourself up to legal action. The bad guys win.

Throwing the baby out with the bathwater

So the very laws that many want put in place to protect us could actually have the opposite effect. It puts the onus on the person installing the software to ensure that they read the terms and conditions of the license agreements, understand what they're agreeing to, and make the decision to install or not to install. And isn't that what we should be doing anyway? Agreeing to an ELUA which entrenches the rights of the spyware purveyor to ensure you don't remove their little piece of the action from your PC just plays into their hands and turns the tables, the victim then becomes the bad guy.

Smarts On Site

E-mail Hoaxes. By Barbara Stuhlemmer, Softdoc Training Solutions

How many have you sent?

We've all received that compassionate message. You know the one. The message tells you of a noble cause and asks for your support.

I receive several of these a day asking me to forward the message to ten other people. Do I participate? No, and let me tell you why.

Continued on page 3

E-mail Hoaxes. Continued...

What is a hoax message?

Basically an e-mail message is a hoax when it asks you to forward it to several other people. Why does this make it a hoax? It is a hoax because it replicates itself logarithmically through willing distribution. Somehow it makes us feel like we will not survive the day if we do not do exactly as it instructs us and pass its message on.

The hoax message comes in many forms. Sympathy messages, jokes, wishes, warm stories, warnings and virus scares. All of these messages prompt us into action to litter the 'Net' with verbal trash.

Are hoax messages dangerous?

They will not crash your PC or bring down your network. Generally speaking it is a harmless message.

So why should we care? As an individual you may not really care about the time you spend reading these messages, but business cares about your time. Every time you open a message that holds no direct value to your work you are wasting your company's time. The accumulation of several minutes a day (let's use 10 for ease of calculation), by five days a week by 50 weeks a year is equivalent to approximately 42 hours a year spent reading and redistributing junk mail. At $15 per hour that is $630 per person. According to Stats Canada there are about 13 million people employed. If only 5% of them are using e-mail at work, that is over $409 Million per year.

If that company is your own you start to feel frustrated by the distraction.

Where do hoax messages come from?

They come from friends and acquaintances that have us in their e-mail address book. The originator of the message is often not known and the reason for starting it can only be speculated. Perhaps someone just wanted to find out how long it would last on the Internet or how many people would read it before they got it back again. Only the originator really knows their reasoning.

How can I tell it is a hoax?

Look for some or all of these signs:

- FW: in the subject line, "Forward" will also show in the body of the message
- Several other previous sender's headings will be in the body of the message
- Subject titles such as "Virus Alert", "Warning", "Joke", "Needs your help", etc.
- The message will not be personalized specifically for you. If your friend the computer wiz and networking guru sends you a message to warn you of a virus, you can bet he is going to start off by calling you by your name and being specific about how the problem is going to affect your system. e.g. "Hey Barb, this is really important for your system…"

What can I do about hoax messages?

Fortunately the spread of a hoax message is completely preventable. Here are some tips.

1. Resist the urge to read the message
2. If you just couldn't resist then do not forward the message.
3. If you find something you feel a friend would truly enjoy, then forward the message, remember to
   3a. Remove the last sender's information
   3b Remove the line at the bottom that requests the message be forwarded to 10 more people.

Ask your friends not to send you these kinds of messages. Tell them you have seen them all before. Let them know they are welcome to send you the short, unique messages only. They are friends after all.

Like 'Snail mail' we learn to recognize what is and what is not valuable. Often we will decide not to open an envelope because we already have enough credit cards, or we never use the coupons. If we spend our time wisely we can free up 42 hours a year to do the things we value more.

Smarts On Site

Spyware ring unmasked.

The image we have of those who create viruses and spyware is usually that of a pale-complexioned socially dysfunctional introvert working for someone who hosts web-sites of a type that I won't mention here. Alternatively the hacker might be envisioned as one who works to be a disruptive force to e-commerce and the global economy. But if we think like this then our stereotypes are showing.

They are villains, of that there is no doubt. They upload viruses, slow down our PCs, make things run slower and increase our frustration levels, but who are “they”?

“They” are not who you might think they are

Well what they're not is pimply-faced hackers with sitting the their parents basements surrounded by Dr. Pepper empties and half-eaten pizzas. The list of suspects reads more like a fortune 500 roll-call. Recently in Israel the top executives of major companies have been arrested or placed on the suspect list of corporate espionage. Companies such as;

- Cellcom
- Yes
- Pelephone
- Meir Motors
- Tami-4
- Ace Hardware
- Volvo Israel
- Amdocs

all have had their executives implicated.

Private Eyes wander the net...

Several private detective companies (scary this) that are run and operated by former Israel Defense Force (IDF) officers have also fallen under suspicion. "If your computer starts to work slowly and you hear your hard drive grinding and working like mad but you see nothing happening on your monitor - you may most likely have an Israel, Syrian, Saudi, Japanese, Chinese or US "shark" spying on your hard drive. It could be the FBI, your mother or the store next door" says Joel Leyden of Israel News Agency.

Read Mr. Leyden's entire article at
http://www.israelnewsagency.com/israelinternetspydefensearrests5540530.html

Don't panic

Please keep in mind that the techniques that the article describes for placing Trojans and viruses on Personal Computers applies to MS Windows, MS Office, Internet Explorer, Outlook, and most probably also an unprotected PC with no firewall and or weak/missing anti-virus or anti-spyware applications. Mac OS X, Linux, K office and Open Office are, by nature, much less susceptible to these kinds of attacks, not impervious, just much less susceptible.

Although the spy-ring was unearthed in Israel you can be sure that this kind of behavior is not limited to any geopolitical boundaries. Remember to practice safe computing.. never open attachments from strangers, close your “preview pane” when using Outlook, have someone check your PCs browser settings to tighten things up so malicious programs can't be launched just by visiting a web-site. Turn on your file-extensions in Windows Explorer (hint: if you can't see the “.doc” of an MS Word file then the extensions are turned off), and keep your spyware, anti-virus programs, and software firewall up-to-date. If you use hi-speed Internet (cable or DSL) I advise you purchase a router and have it's firewall activated to give added protection.