

YOU HAVE BEEN HACKED! (GET USED TO IT)



Richard W. Schierer
September 2011

Every computer that you own or use at work has been hacked in one form or another.

Whether by a professional hacker or by a co-worker. Hacking is defined as, “someone who breaks into computers and computer networks. Hackers may be motivated by a multitude of reasons, including profit, protest, or because of the challenge.”

Now that you know ‘what’ a hacker is and what motivates them, you can understand why I said in the being that every computer has been hacked in one form or another. Every government, large and small has been hacked. Every company, large and small as well. Other countries, businesses and organizations have agencies or groups of people whose sole purpose in life is to ‘hack’ or break into your computer systems and take a copy of your precious data. This precious data takes many forms. If you are the Department of Defense, you have security plans for every operation around the world. If you are one of their contractors, who job it is to create the next generation of jet or rifle or missile, you have working plans, diagrams, budgets and insider information about these projects plus what you know about your competition.

But what if I am just a little 5 person company or work from home? What data or services do I have that they could possibly want? What they want from you is not your data. What they want from you is to control your computer and turn it into a ‘zombie’.

In computer science, a zombie is a computer connected to the Internet that has been compromised by a cracker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

(courtesy http://en.wikipedia.org/wiki/Zombie_%28computer_science%29)

Your computer, whether at home or at work may have been taken over by a virus which has loaded some code that instructs it to perform certain things when it receives a signal from its creator. What could a computer do that has been infected with this code and turned into a zombie do you may ask. Not much, but considering that 10’s of millions of computers are unknowingly infected with viruses and are now zombies, they could do a lot!

Let’s say you are a hacker whose ‘job’ it is this week to affect Macy’s ecommerce website and it just so happens that it is the busiest week of the year, the week before Christmas! You as the hacker, send a signal to all your zombied computers which instructs them to try to access the Macy’s website. You know what it is like when a website you want to access is slow...? Well when a hacker launches a Denial of Service Attack, he tells his millions of zombies to access Macy’s and constantly request information. Macy’s computers become so overwhelmed that their server not only slows down, but crashes! Macy’s is losing millions of dollars a minute in ecommerce sales due to their website being down. Their

IT staff works frantically to resolve the problem but can't due to the multitude of 'hits' the website is taking. Only when the hacker tells his zombied PCs to stop will Macy's IT staff be able to resolve the problem, but not without Macy's have lost millions of dollars in the process.

We all know how many viruses or stories about viruses affecting the Microsoft Windows operating system there are. Hackers attack Windows because 90% of all computers have Windows on them and by writing code to affect Windows, they get to get their message out there. And then there are the hoax viruses which are the hackers spreading SPAM around indicating that a lethal virus is going to hit on a certain date. When in fact they are just spreading rumors and gaining headlines.

What is a computer owner/user supposed to do. Well get used to it. As time goes on, attacks will come in new ways. Be delivered in new forms (Hey! I just found this USB stick in the parking lot, let's see what is in it!). Emails will direct you to malicious websites which are not the ones you think they are and you enter the requested information into the website, like your bank account id and PIN. That is called phishing and know what? If you did this, you just lost all the money in your bank account!

There are many ways to protect yourself from being hacked or from getting viruses. The most important one is to be educated about them. Don't open every email that you receive. Don't forward the ones you open to 100 friends so you will get a good surprise in the morning! Don't do anything without thinking about it.

There are a few places that you are guaranteed to get viruses from:

1. Your email
2. File sharing sites, where you get free music
3. Porn sites

If you are a business or home professional you need to have a talk with your IT professional. Please feel free to write us at rich@makemytechnologysimple.com or call us toll free 800-918-7390 with any questions you might have about this article or computer technology in general.

Let be safe out there!



Richard W. Schierer

makemytechnologysimple.com

631-375-4512