

February 2012

ITR Technologies, LLC
"Serving All Your Computer & Network Business Needs"

Tech Talk



We <3 Our Customers!

We all have busy lives, and sometimes we don't take enough time to acknowledge the ones who are most important to us.

This Valentine's Day reminds us about those who matter most - our customers! We're always grateful for your business, and thankful that you entrust us to provide for your tech needs.

Hope we remain Valentines all year round!

Virus, Malware, Spyware, Oh my...

In the current age of global economy, no business can afford to be without access to the Internet. Unfortunately, there are a growing number of threats that cause headaches and frustration to novice and professional users alike. Below is a list of the 5 most common things that I hear when a client has an infection.

1. **"But I have a firewall"** – While a firewall is an essential part of any business network, its function is often understood incorrectly as the ultimate protection from the outside world. This isn't really the case. The function of a firewall is to protect your network from outside intrusion. Your internet router is a door, and the firewall is the security guard asking if incoming traffic has permission to be there. Instead of just a simple firewall, you might consider a Unified Threat Management (UTM) device. There is an additional cost, but UTMs

— Scott Bernstein

enhance the protection of the network by combining the technology of antivirus and even antispam with a firewall. They not only ask whether the traffic is allowed in, but also what kind of traffic it is.

2. **"But I have antivirus"** – Antivirus software is similar to the inoculation shots we all received as a child. First, the infection was identified. Then the cure was developed. And, just like the flu every winter season, as the strain of infection changes, a new cure needs to be created. One of the biggest things that can help is to make sure that your antivirus software has current definition files, and that the software is up-to-date. Using Norton or McAfee 2009, even with the most current AV definitions, will not be as effective as the current software version and today's definitions.

(Continued on page 2)

Expert's Corner: Thy Buffer Runneth Over

This month we'll look at a particular weakness that can be exploited by hackers, the Buffer Overflow. It's something you've probably heard of already. But you might not know exactly how it works, what the risks are, and how to protect yourself.

What exactly is a buffer overflow? To answer this question, we have to understand a little bit about how computer programs use memory. A computer program consists of two things: 1) A set of instructions, and 2) A set of data that those instructions will operate on. Normally, all of the instructions are loaded into memory when the program starts. Data comes in from some input source, either disk, a user interface, or the Internet, and gets stored in memory temporarily so that the computer instructions can use it. Finally there is some output data, which is created

within memory and then moved to an output device, which again may be a disk file, a user display screen, or the Internet.

The program has to arrange for a place within the available memory to store the data. You might think of computer memory as a plot of land, with different sections separated by fences. The computing instructions go into one fenced-off area. From there, they direct the data into, and out of, a different fenced off area or "corral". So what happens if some of the data decides to jump the fence, and trample all over the instructions?



(Continued on page 2)



Virus, Malware, Spyware, Oh my...

(Continued from page 1)

3. **"I didn't do anything, it just installed itself"** – While this statement may seem true, most current infections require some sort of user interaction, even if we were completely unaware of it. Attackers insert their infections and malicious code into everything from hyperlinks to even web images. The act of clicking on a picture on the internet can launch code that installs the infection into your computer. The code may even have a time bomb aspect which delays the infection so that it becomes harder to track the source of the malicious code. It also gives the infection time to insert itself into your computer's restore points and backups.
4. **"I don't go to those kinds of sites"** – Malware and Viruses can be found nearly everywhere, embedding themselves into any picture, icon, or link on the web. The use of Site Advisor software may help mitigate this threat.
5. **"I knew the person who sent the email"** – This recently caused issues for some of my friends. My Yahoo account was

used to send an email containing an internet link that took users to an infected site. This email was sent to people in my address book at 2:30 AM on a Friday night, which is not a normal time for me to be sending emails! Most of the people who received it realized it was malware and deleted it right away. Others saw the subject line, which said "About your stomach problems", and realized it didn't apply to them. Finally, some people noticed that the only text in the email was the internet link and nothing else. For the one or two people who were tempted to open the email, this was the final red flag that scared them away. So when opening an email, remember these guidelines: First, see who it is from, and avoid opening emails from unknown senders. Second, check when was it sent - is this a time when that person would normally be sending me emails? And finally, look at the content of the email - is it something that this user would send me?

You do not need to be a rocket scientist to protect your computer; just be vigilant and use common sense (which often is not so common). If you don't, you will have to call the Wizard to get rid of the evil witch that infected your computer.

Thy Buffer Runneth Over

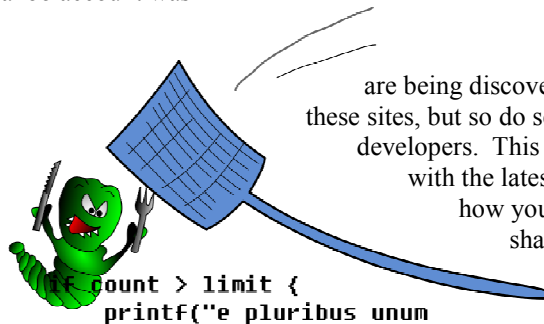
(Continued from page 1)

Luckily, data doesn't have a mind of its own. But, suppose your program doesn't have a very good fence. Or, suppose the programmer drew a line in the dirt where the fence was supposed to go, but forgot to actually build it. Then, suppose you get some data coming in that doesn't fit inside the corral. It's going to overflow right into the instruction area.

If this happens by accident, the most likely outcome is that the program will either freeze or just crash. There's also a chance that nothing strange would happen, if the data overwrites some instructions that are not going to be used. But there's also a slim chance that the data might be interpreted as program instructions, and cause the program to do something it's not supposed to.

Enter the hacker. If someone knows enough about the structure of a program and the operating system it is running on, they can predict the "size of the corral" that is supposed to hold the data. They can also tell the exact place in the program instructions where they could intercept the program flow. Then, they can craft some input data that is bigger than it is supposed to be, but is just the right size to "jump the fence". They add some special instructions in just the right place. They send the data to your program, where it leaps into the program instruction area and it takes control of your computer.

If this sounds scary, then I've succeeded! It's easy to find instructions on the Internet to take advantage buffer overflow vulnerabilities. Websites like packetstormsecurity.org and exploit-db.com list updates on new vulnerabilities that



are being discovered every day. Hackers monitor these sites, but so do security professionals and software developers. This is why it is vital to always keep up with the latest patches and security upgrades. It's how you can keep your fences in good shape, and the data in the corral.



February 2012

**1455 Highway 6 South
Suite B**

Sugar Land, Texas 77478

(713) 344-1618

www.itrpro.com

***“We make all of your
computer problems go away
without the cost of a full-time
I.T. staff”***

Ask us about our fixed price service agreements — Computer support at a flat monthly fee you can budget for just like rent!

Inquiring Minds...

As new cell phone technology becomes available, businesses trend toward obtaining the latest and best available. In an effort to be as efficient as possible, we now use cell phones to power our businesses and to engage with clients through email, twitter, and other useful functions.

But did you know, an estimated 500,000 cell phones are discarded and thrown into the trash every day? These cell phones become pollutants that are dangerous to the environment.

What can businesses do with their old cell phones? Instead of throwing them away, a business can leverage the power of the cell phone with help from organizations like George Washington University. At GWU, student organizations have committed to collecting 20,000 used cell phones. In cooperation with Hope Phones, the cell phones will be recycled or sold for parts, and the proceeds used to provide new cell phones to those in need around the world.

Through this program, GWU students hope to provide cell phone access to women in the Republic of the Congo and Nepal, and to spur innovation and investments in technology projects in these two countries. By donating old cell phones, businesses can help the environment and also receive a nice tax deduction. Please visit www.gwu.edu/donate-phones or hopephones.org for more information on how your business can donate cell phones to a good cause, while spreading health and love this season!

Do you have an idea worth spreading?

“TED (Technology Entertainment Design) Talks” is a bi-annual conference that brings together the most fascinating people on the planet to share their ideas in a memorable talk with the public. The videos are free to watch on the TED website or podcast. The topics range from breakthrough research to modern technology to cultural ideas.

TED Talks are designed to encompass a wide range of ideas that can help initiate change. Past speakers include

— David Do

Al Gore, Bill Clinton, Bill Gates and Malcom Gladwell. To inspire a new generation of thinkers and doers, TED offers an annual award to a chosen winner who presents their "One Wish to Change the World". The winner receives \$100,000 to fulfill their wish.

The motto of TED Talks is "ideas worth spreading". On their website ted.com, anyone who has internet access can view videos of individuals giving the talk of their lives, about subjects that they are experts in. There are over 1050 talks available, and as of June 2011 the videos had been viewed over 500 million times. The popularity of TED continues and expand into other countries. Today, they have annual conferences across the world.



Happy Valentine's Day! 

 **We Our Custom-**

713-344-1618 x151