**Malvertising… again**

You know those little ad squares that appear on popular websites? What if those little squares could be used to distribute viruses? Well, that is the very definition of "Malvertising": Malicious software and virus code inserted into popular websites via the ad boxes on the site. You surf to the site, click the ad, and Boom! You are infected.

Here is an article from Tom's Hardware website that explains Malvertising better than I ever could:
http://www.tomsguide.com/us/malvertising-what-it-is,news-19877.html

Malvertising is on the rise, unfortunately… for various reasons:

1. Email has become harder to infect – firewalls, anti-virus software, and careful, educated computer users have become much better at recognizing attachments that don't seem right, sketchy web links, or just plain odd. So the virus writers and distributors are moving to an easier target: web browsing.
2. Java and Flash software (which are vital to websites) are still weak links – both are riddled with bugs, vulnerabilities and just plain gigantic security gaps.
3. Website operators are desperate to fill ad slots on their sites, and have dropped their guard (and perhaps their standards) on whom they accept as advertisers on their websites. Automated ad systems make things even worse because there is no human involvement/review at all.

A recent study concluded that email is no longer the main vector for virus infections, that title now belongs to web browsers: possibly up to 75% of infections are attributed to web browsing:
http://www.darkreading.com/browsers-are-the-window-to-enterprise-infection/d/d-id/1318906

**What to do? Two Steps:**
#1 – One major issue is that your user account is probably an administrator-level account. Administrators can do anything, which includes inadvertently installing viruses. You can eliminate this problem by creating a new "Standard User" (non-administrative) account on your computer - here's how:
http://windows.microsoft.com/en-us/windows/create-user-account#create-user-account=windows-7

#2 – Piggyback that with an additional step to disable all add-ins, plug-ins, and add-on apps in your browser. Usually, it's the plugins and add-ons that open the door to vulnerabilities. Here's how to disable the plugins:
http://www.howtogeek.com/139916/how-to-view-and-disable-installed-browser-plug-ins-in-any-browser/

Now you have a safe/secure user account with which to do your recreational surfing. Yes, it is a bit clumsy to have to switch between user accounts just to surf the web, but it is more secure than doing all surfing on an administrative account.

-John Becker


Phone: 630-852-1736 john@medofficesystems.com Fax: 630-214-4565