Nov. 01, 2007

In last month's column (www.CPATechAdvisor.com/go/1761), I discussed web advertising, its four basic components and how it works. As you may recall, the four most common types of web advertising include the following:

- Click-Through Advertising
- Direct Advertising
- Internally Developed HTML Formatted Unsolicited Commercial Email

I also defined each of the forms of advertising and discussed how each is distributed. This month, we are going to turn our attention to how this malicious web scripting can be embedded in web advertising in order to infect a person's computer with a Trojan software program that enables one to steal information or control the computer.

Things You Can Do To Prevent Infection

As you gear up for tax season, consider spending a few minutes talking about these threats and ways for your accountants to avoid becoming victims. Several things can be done to prevent infection. In my September column, I listed several ways to prevent JavaScript attacks, which are also very applicable to web advertising attacks. These preventive measures and some new ones include the following:

- Institute an Internet Policy in your firm that bans the use of non-work related sites.
- Educate employees on the potential problems that might occur from visiting non-work related websites such as YouTube using work computers.

- Make sure you use Internet site security controls and other content control

products updated.
- Use a managed service content filter provider who screens both e-mail (to remove unsolicited commercial e-mail) and website content (for malicious code). MX Logic is one company that offers this combined type of service. Many providers
in this space offer either unsolicited commercial e-mail filtering or web content scanning, but not both. When considering a service, make sure they can do both, as it helps to eliminate the threats in your environment.
- Use a firewall that also offers intrusion protection scanning and monitoring. The Cisco ASA 5510 and higher models offer an intrusion prevention module. SonicWall also offers an intrusion
detection and prevention module on its devices. These devices scan the content coming in from the Internet and block content that is not appropriate.

Why This is Important to Practicing Accountants

Before I get into how web advertising can infect your computer and what to do about it, let's take a look at why web advertising and JavaScript hacking
are important to you as a practicing accountant. Why do you need to worry about these problems when they have nothing to do with preparing tax returns or performing
an attest service? And if it's not something that's going to help
your practice, why would you bother learning about it? The fact is, there are some very important reasons why this is an important issue to you as a practicing accountant:

- You need to protect your clients' financial information.
- You need to prevent your computer systems from being compromised by viruses and malware. A compromised computer can be used to send spam, attack other computers, participate in denial of service attacks, host illegal copies of

software or, worse, be used by child pornographers to distribute their illicit

An infected computer can cause a large amount of damage to your firm in terms of image and lost productivity. An infected computer allowing a hacker to steal your entire set of client financial information might be a serious problem. Now that we know what we are faced with as practicing accountants, let's take a quick look at how this advertising works and then get into figuring out how to fight against this threat.

How Click-Through Advertising Works

Before I explain how the content is delivered, let's take a look at some terms with which you need to be familiar:

- **Advertiser** — The company providing the content.
- **Click-Through Provider** — The company responsible for providing the HTML code to display the advertising content, tracking the number of clicks on the content from the sponsor's website, and providing payment to the sponsor. Microsoft, Yahoo!, and Google all have subsidiaries, divisions or third-party providers under contract who provide this service on their company-controlled websites as well as selling content directly to sponsors.
- **Sponsor** — The company or website signing up with the click-through provider to provide the advertising on their website. Anyone with a website can sign up with a click-through provider to obtain advertising content for their own website. The only requirement is that they have the ability to insert the HTML code into their website.

A company wishing to promote its product or website signs up with a company that provides click-through advertising content defined here as the click-through provider. The advertiser provides the click-through provider with the content to be displayed on the website. The sponsors who sign up to provide the advertising

on their website place special HTML code on the sponsor's website. When

column, it may also be other code that can be executed on your computer. Computers with unpatched vulnerabilities are especially susceptible to other types of coding besides JavaScript. Once the script is successfully run on the computer, it will be designed to bring down other components, which are also installed on the computer. This will either place the computer under the control of the attacker or the attacker will steal information off the computer, which is then sent back to the hacker or huckster.

Additional Protective Measures

In addition to the items outlined below, additional protection can be obtained by actively using the site settings functionality in Internet Explorer via the Security Tab in Internet Options. Mozilla, Firefox, and other browsers offer similar functionality in their products, as well. Because I'm most familiar with Internet Explorer, those are the settings I will discuss here. However, feel free to use the concepts here to implement content control in your favorite browser.

Much of the web advertising content can be locked out by simply using the concepts of trusted sites in Internet Explorer. One of the key components in last month's column was pointing out that all web advertising content is going to be coming from a website other than the one being visited. By simply raising the level of your Internet site zone security settings and using the trusted sites settings functionality to trust sites that you are visiting, you can block 99 percent of the web advertising content. An example of this is Sun Microsystems' Java website: The main website is www.java.com, but all the advertising on the site comes from http://ads.sun.com. If you put java.com in the trusted sites and raise your Internet security level, the ads.sun.com will be blocked from displaying because they are not part of a trusted domain. (See my April/May 2007 column, "Internet Explorer 7: Finally Creating

A Safe Browsing Experience," at www.CPATechAdvisor.com/go/1515).

to help in the prevention of web advertising and JavaScript infections on the computer. However, be careful of making too many changes at once because you could really degrade your browsing experience. Too many changes can become difficult
to reverse because you may not know which one to undo in order to return to the way it previously functioned. Turning off JavaScript execution in advanced settings is one of the best ways to prevent this content from being harmful to your computer. Content filters are an additional way to block web advertising infections.

Virtualization Can Help

Virtualization can provide a means of allowing you and your employees to access the Internet for both personal or business needs without worry about impacting your office or your operations. By using either Microsoft's Virtual PC 2007 or VMWare's VMWorkstation, you can set up a second PC running on your computer — a virtual machine that uses the resources of your computer to run a second computer. You can then use this second PC for browsing the Internet, and it won't matter where you go online. If the machine becomes infected, you simply erase the virtual machine and create a new one. In my December column, I am going to focus more on the virtues of virtualization technology along with the security benefits of using virtualization.

Web advertising is just another in a long list of infection mechanisms of which we must be alert and recognize when using the Web. Unfortunately, not many tools are currently available to help keep the denizens of the Internet from using web advertising and JavaScript to penetrate our computer systems and cause problems. Fortunately, these new attack tools are still early in their development and not widely used since other means of infecting computers are still available. There is, however, a growing increase in web advertising attacks

via e-mail as more and more people become infected with the latest worm as of

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.