From the Sept. 2007 Issue

One of your employees at home is browsing the Internet and finds a cool video on YouTube. They decide they want to share it with all their coworkers because it is so funny. They send the link into the office. The next morning, they distribute it to their coworkers who dutifully view the content. On the surface, this may seem like a very benign issue with all the antivirus, anti-spyware, firewalls, and other stuff we have installed to protect our computers from various attacks. For many of you, this may just seem like another easy day at the office with a few coworkers sharing a funny video. Well, perhaps it seems that way, but the reality is that it may not be that simple.

An article about Web 2.0 vulnerabilities crossed my desk the other day and made me rethink the above scenario as perhaps not being as benign as it first seemed. As I began to more closely examine the situation, I became more and more concerned about its impact on accounting firms. Many web browsers, by default, allow JavaScript to run. Mozilla Firefox takes a slightly different approach and allows JavaScript to run on a site-by-site basis if the user trusts the site and approves the JavaScript to run. However, this offers little protection since most Web users have little knowledge about what they are approving to run.

This is the "gotcha" of Java-Script hacking. By putting JavaScript code into a Web 2.0 site, a hacker can very quickly and easily get a user to run the code and install something they do not want on their computer. I will delve into this in more detail later in the article, but let's first run through some definitions so we are all current on the latest technical speak.

Definitions:

Web 2.0: In the past few years, several new Web formats have come into

(web) pages, which are otherwise static, since HTML is a display language and not a programming language. JavaScript is easier to use than Java, but it's not as powerful. It is used mainly to deal with elements on the web page.

What is Malicious JavaScript?

Malicious JavaScript is any type of JavaScript used on a website that installs software or obtains information from the computer without the user's knowledge. Let's take a look at some examples:

Example 1: A malware author could place JavaScript code on a web page that directs the browser to a specific URL under the malware author's control, which loads additional JavaScript code into the browser. This code could do anything the author desires such as scanning the user's bookmarks and cookies, harvesting them and sending them to the criminal's computer without the user knowing. While this may seem innocuous, remember that many users in their browser select the option to have the browser remember the usernames and passwords to specific sites visited by the user. The criminal, having downloaded the cookies from the user's computer, simply needs to identify the one associated with the user's online banking account in order to gain access to the user's bank accounts.

Example 2: Gaining access the same way as in example one, the malicious hacker instead substitutes the host name of a URL stored in the user's bookmarks to a website under the control of the criminal. The criminal's server will then offer up a phishing page that requests confidential information from the user. Believing they are on a legitimate site, the user will generally enter this information, especially since the user launched the

website from their Favorites list after previously adding the site to their

JavaScript code in a web page. Now, let's take a quick look at an example of how this has already occurred. Earlier this year, using an exploit in the Vector Markup Language (VML) on Microsoft Windows-based computers, cyber criminals infected the Miami Dolphins' stadium website just prior to the Super Bowl with malicious JavaScript. The malware authors were able to use this vulnerability to load malicious JavaScript onto the website. This allowed them to infect other VML vulnerable computers. The JavaScript downloaded a Trojan, one of the ZLOB variants, which further downloaded other malware used to steal World of Warcraft accounts.

The Impact

All of the Web 2.0 site types defined above use various forms of JavaScript to produce and display the content on these sites. Since many of these sites are user-controlled (i.e., the user is responsible for adding the content), it would be very easy for someone to create a cool video on YouTube and post it along with some JavaScript that infects the computer when the video is played. Blogs, Wikis and all of the other new content that falls into the Web 2.0 definition are vulnerable to someone using such avenues to introduce malware into the computer. Most antivirus and anti-spyware applications do not scan web content for malicious JavaScript.

Protection from Attack

Since JavaScript is embedded in HTML coding (the language used to display websites), it is not a simple matter to disable all JavaScript in your browser. Some sites require JavaScript to function properly and to accept user input. A form website is an example of a JavaScript-enabled website. Certainly, some users in an organization may not need to visit sites that have JavaScript, and their browsers could have the JavaScript disabled. But for many of us in the accounting profession, it is difficult to avoid websites that require us to fill out forms and other information in order to help our clients. JavaScript is an essential part of these websites and is something that we have to use.

JavaScript is a threat to your office computers in ways that you may not think about

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.