TECHNOLOGY

Web Ads: A New Virus Delivery Method — Part I

Column: The eSecurity Advisor

Oct. 01, 2007

From the Oct. 2007 Issue

In last month's column, I took a look at JavaScript and how it is being used to infect computers and steal information (www.CPA TechAdvisor.com/go/1663). In a two-part column starting this month, we are going to examine another process that is also allowing hackers and hucksters to infect computers and steal information. This particular process uses web advertising content delivery to infect unprotected computers. As if we didn't have enough to worry about in running our accounting practices, now we have to worry about visiting even legitimate websites and our computers becoming infected with malware.

How Web Advertising Works

Web advertising works by the host site putting in HTML code (the programming language used for displaying web pages) that displays the advertising on the website (usually in line or on the left/right of the page). When a user clicks on this content, they are taken to a new website, which is generally not the same site they were viewing. In order to make money in web advertising, there are many different models that have become available. The most common types of web advertising include the following:

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

Defining The Types of Web Advertising

We won't concern ourselves with two of these methods for purposes of virus delivery — direct advertising and internally developed. However, just so we have a definition of each, let's quickly define them.

- **Internally developed advertising** is content developed internally by a company for use on its own website to promote other parts of the company. Since most of this content is developed in-house, its threat to your computer is minimal if you are visiting legitimate sites. Phishing sites, which are specifically designed to entrap a user, would be the exception.

- **Direct advertising** is the sale of advertising space by content companies, which is directly solicited by the company. Microsoft, Yahoo!, Google, and Amazon all solicit either directly or through subsidiaries for advertising content, which is an example of this type of advertising. Since these companies control the content on their site directly and work directly with the advertiser providing the content, this type of content generally is not going to be an infection source. It should be noted that some big companies use various methods of obtaining web advertising including some of the higher-risk methods. Just because you are on a trusted company's website, does not mean you can let your guard down. Direct advertising is difficult to differentiate from the other sources of advertising because the delivery method is very similar.

- **Click-through advertising** is the most common and oldest form of legitimate advertising on the Internet. As with most of the significant advances on the Internet, the pornography industry was heavily involved in the early years with the development of this advertising delivery system. They needed a way to get their sites advertised, and traditional means of advertising were generally unavailable to them. The pornography industry needed a way to pay for the advertising so they developed third-party companies to handle the content delivery and payments. These related companies and others seeing an opportunity eventually branched out into delivering other types

of advertising besides pornography. Click-through advertising is integrated into a company's website after the company signs up with a provider to deliver advertising content. The company signing up with the advertiser then positions special HTML coding into its company website to display the advertising either on a static basis (the same advertising over and over for each viewer) or dynamic basis (the content changes each time the page is viewed or refreshed). When a viewer of the site clicks on the advertising content, they are taken to the advertiser's website, and the provider (the person who allowed the advertising on their website) gets paid some money when one of two things happens — the person either buys something from the advertiser's website or the advertising campaign simply pays a few pennies per click to the provider for providing that advertising content to the viewer. It is very important to remember that the advertising content is provided from a different website than the company's own website. This fact will be very important as we discuss how to prevent this advertising content from infecting your computer.

Early Click-Through Fraud

When click-through advertising was first developed, hucksters and hackers quickly figured out a new means of making money. Early hackers figured out that if they wrote some simple code to open a link to a click-through site that they posted on a website they controlled, they could make a large amount of money by using those automated tools to click on the link hundreds or thousands of times. Because a computer can perform a task much faster than a human can, it could create hundreds or thousands of clicks per day. At even a penny or two per click, a few 100,000 clicks can add up to big money in a hurry, especially if done over a period of a few days or weeks. Companies quickly caught on to this and started using tracking cookies to ensure that purchases were made before payments would be received or to determine if the user had already visited the sites.

An arms race of sorts ensued, where the industry and the hackers and hucksters figured out ways to work around the new processes put in place to prevent fraud. Early click-through fraud is one of the primary reasons we now have the funny looking characters on ticket purchase sites and other websites where they want to verify that a human is present. Even early versions of this technology have been replaced by more complex forms as the arms race continues (although it has slowed in the past few years as the hackers and hucksters have not been as quick to figure out workarounds to this technology). This latest security

procedure is an example of the technology development that grew out of early click-through fraud and ticket purchase fraud.

Unsolicited Commercial E-mail

With the integration of HTML coding into the Microsoft Office Suite, e-mail became a new advertising dream for the hackers and hucksters who use web advertising as a means of infecting computers. The Unsolicited Commercial E-mail (UCE, also known as SPAM) senders quickly adopted this technology into their processes since it makes it much easier for them to induce the unsuspecting into clicking on a link or simply using the content as a means to directly infect a computer. There are two broad categories for UCE:

- Fraudulent e-mails, and
- Non-Fraudulent e-mails sent in an annoying way.

Fraudulent UCE is designed to induce the user into clicking on a link or other web-enabled (HTML) content in the e-mail for purposes of stealing information or infecting the computer with malware. Non-fraudulent e-mails sent in an annoying way are designed to induce the reader to click on web-enabled (HTML) content for purposes of selling the user something in an unconventional way because it is close to or just barely crosses the line between legal and illegal. This type of advertising is the easiest of the web advertising types described for hackers and hucksters to use to get the unsuspecting to visit a website under their control. Once they have the person under their control, they can then use JavaScript attacks or additional advertising content with embedded malicious code to further infect the computer. Generally, the fraudulent type of advertising is the type that must be watched for and is the one most likely to infect a user's computer when visiting one of these sites. Users may intentionally be misled into clicking on the content or may unintentionally click on the content when trying to clear UCE from their e-mail.

Summary

We now have an understanding of the types of web advertising and the means of using it to infect a computer. In next month's column, we will examine some ways to prevent these types of things from happening to you … especially ways to prevent bad things from happening on websites you trust or that seem trustworthy. We will also discuss ways to address those times when you

unintentionally
click on something and end up on one of these sites.

Technology • Article