Zeus Computer Virus Threatens to Steal Identities of Online Shoppers - An ACCESS Fraud Alert

December 13, 2010 - This year, millions of Americans will choose to do much of their holiday shopping online. In prior years, one of the best ways to remain safe from fraudsters was to do your online shopping on well known websites. But the Zeus Botnet - which is technically known as a Trojan Horse - has changed that. If your computer has been infected with Zeus, then you run the very serious risk of having your identity stolen even on some of the country's best know websites, unless you know what to look for.

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

The initial targets for Zeus have been Macy's and Nordstrom's websites, but computer security experts expect that to change relatively quickly. This iteration of Zeus - which has been around for quite some time - is both simple and ingenious. It inserts a pop-up window when you visit a targeted retailer's website that appears to come from the parent site. It asks for credit card information, Social Security numbers, mother's maiden name and your date of birth. Virtually everything needed to walk away with your identity.

Computers can become infected by visiting infected websites, clicking on unrecognized links in e-mail messages, or simply hooking your computer up to an infected portable storage device or USB drive. And because Zeus can be used to target any website, it is only a matter of time before people with infected computers start to see these pop-ups appearing at other retailers sites. It is also likely that the program will start to appear on banking websites.

The best protection against this program is to make sure that you have antivirus software installed on your computer and that your virus definitions are up to date. When visiting any website, consumers need to be aware that no legitimate e-commerce or banking site is going to ask them for their Social Security number. Any consumer who has this information requested of them should make a note of the site they are visiting and notify the operator of the site. They should then immediately have their computer swept for viruses. Under no circumstances should they attempt to make online purchases or conduct any online banking prior to having their computer cleaned.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter: