2/9/2010

Bulletin 2010-001

Internet Browser Malware Targets Internet Banking Users

Malicious software targeting Internet Banking users is evolving and on the rise. These malicious programs are commonly known as Internet Banking Trojans. Some examples of well known Trojans include Zeus (also known as Zbot) and URLzone. According to Anti-virus reports, Zeus accounts for up to 44% of infected systems. The malware places the victim's computer into a network (Bot Net, Bot Network) of infected systems making outbound connections to servers controlled by hackers. The victim's infected system downloads additional viruses and malware for the purpose of capturing sensitive information; such as logins to an Internet Banking Web site. These exploits rely upon the victims being inadequately protected by up-to-date virus protection software.

The "man in the browser" attack is one of the most dangerous techniques used by the malware which is similar to a phishing attack. This attack occurs when the user visits and logs into an Internet Banking Web site. The malware then injects a Web page into the victim's browser and modifies the URL so that it appears to still be connected to the Internet Banking Web site thus tricking the user into believing the page is legitimate. This is a very sophisticated and tricky tactic since the URL still shows the Internet Banking Web site.

The infection techniques are similar to other types of malware which is captured through spam, phishing emails, and malicious Web sites. Attackers are also targeting users of Social Network sites to spread these malicious programs.

Actions and Recommendations:

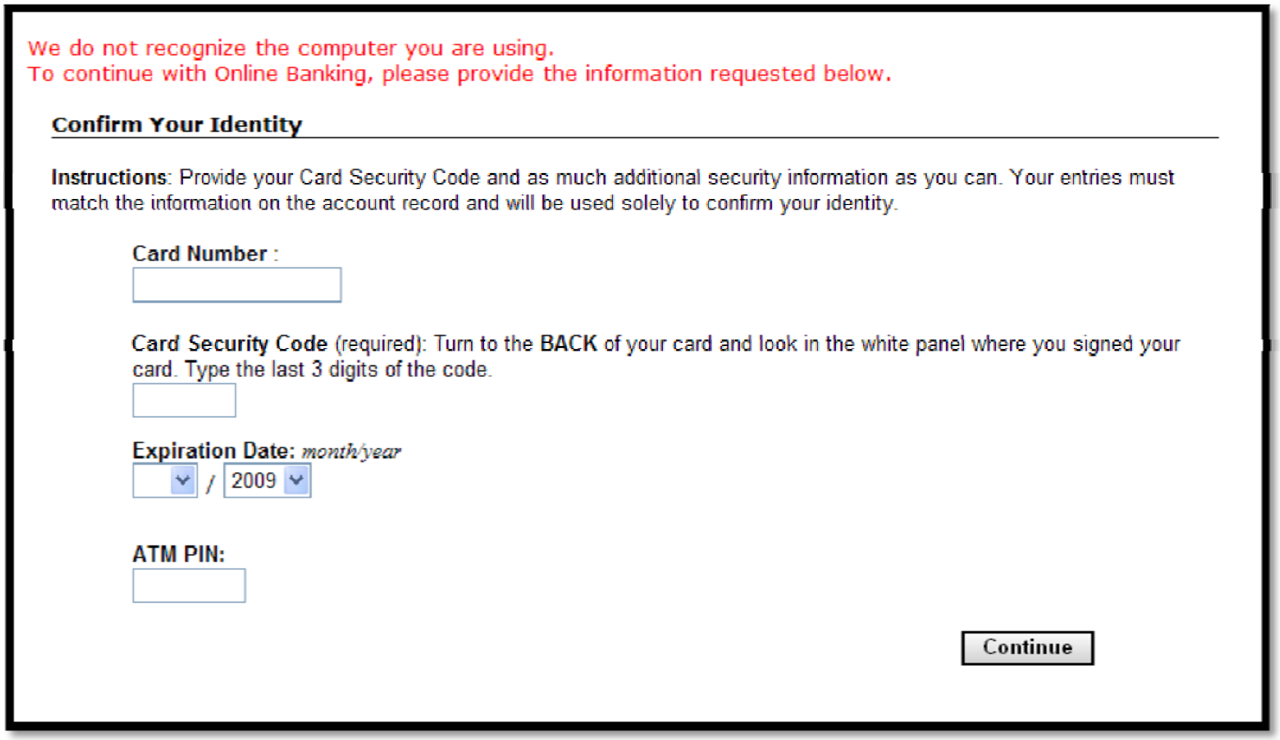
Security Awareness is the best defense for your members. If you already have a procedure for notifying your members of viruses and phishing emails, then it is recommended to use the same approach. However, this particular threat should come with a critical warning notification.

The following could be used as an alert:

Security Alert – Viruses asking for Credit Card or other Banking Information

Viruses and other malware are targeting online banking users. These viruses may create a Web page that appears to be part of your credit union's Internet Banking Web site. The Web page will look very generic and will most likely not have the credit union's name or icon on the Web page.

The page may appear similar to the following:



We do not recognize the computer you are using.
To continue with Online Banking, please provide the information requested below.

Confirm Your Identity

Instructions: Provide your Card Security Code and as much additional security information as you can. Your entries must match the information on the account record and will be used solely to confirm your identity.

Card Number :

Card Security Code (required): Turn to the **BACK** of your card and look in the white panel where you signed your card. Type the last 3 digits of the code.

Expiration Date: *month/year*
/ 2009

ATM PIN:

If you see a Web page similar to the one above, follow these procedures:

1. Notify your credit union immediately if you submitted your credentials, Credit/ATM Card Number, PIN, or any other sensitive information.

2. Re-install your Operating System or work with a PC specialist. You may also contact your PC vendor and Anti-Virus Vendor for advice and assistance. Please Note: If you attempt to remove the Virus, make sure to follow the instructions posted on an Anti-Virus Vendor Web site or contact them directly for assistance. They will most likely recommend a new installation since they will not be able to guarantee their program to completely remove all traces of the virus. Remember- If you back up your “My Documents” and other files, the viruses could be attached or located within these files. Make sure you scan these files before opening again on the newly installed system.

3. Purchase a new Anti-Virus Software program or re-install your Anti-Virus program. Make sure you configure the program to check for updates daily. Your Anti-Virus software should also be configured to protect your computer from Spyware, Internet Browsing, and Multi-Media programs. If your Anti-Virus program does not include these protections, it is critical to get these additional features or find an upgrade to another version that does have these protections.

4. Make sure your computer is configured with at least two user accounts. The default account has administrator rights. If you use the default account, viruses may be able to modify your system files by using this account. If you create another account that has basic computer privileges, this may help prevent viruses from making system modifications. This will help prevent attacks that Anti-Virus software has not yet identified.

5. If you have two computers, we suggest using one for Internet Banking and the other for casual browsing. If you only have one system, then use caution when visiting Web sites, especially Social Networking sites. These sites are primary targets for hackers. Other sites may also be infected by hackers such as software download sites. If you download a program, picture, or some other file, right-click on the file and select scan with your Anti-Virus program before opening or running. It is always better to select “Save As” instead of “Run” when downloading a file or program over the Internet.

Identity Theft and Red Flag procedures:

If a member calls to inform the Credit Union of their personal computer being infected and the member submitted their Credit Card or other sensitive information as a result of this malware, you will need to initiate your Red Flag/Identity Theft procedures. Some examples of procedures you may include in your Red Flag procedures:

- Canceling their ATM or Credit Cards
- Contacting the Credit Bureaus to place alerts on the victim’s Credit Report
- Advising the member to visit the FDIC’s Web site for Identity Theft guidance
- Changing their account logins
- Disabling their Internet Banking access temporarily
- Monitoring their banking transactions closely
- Placing an alert under their member account so the Member Services team and tellers ask additional identification questions when the member calls or visits

- Discontinue certain transactions over the phone and over the Internet such as Wire Transfers, Bill Payment, and Remote Transfers.
- Monitoring the member's changes online or over the phone requests such as Change of Address, Change of Phone Number, or Change of Email.

Questions that may be asked by the Member or Account Holder:

Is the Credit Union's Web site infected?
Answer- No. The virus is being spread through social networking sites, emails, and free software download sites. The virus is loaded and runs on the user's personal computer and appears to the user to run on the Credit Union Internet Banking Web site.

Why does my browser show the correct Credit Union Web address when the fraudulent page is displayed?
Answer – The malware is sophisticated enough to not run until after the user has submitted their login credentials including security images before loading the fraudulent Web page. The malware appends the URL string with a similar string in order to trick the user into believing they are at the correct Web site.

Has my login and password been compromised?
Answer-Our assumption is yes. The virus may contain a key logging program, which sends login credentials to the attackers' server over the Internet. Notify your credit union immediately so they can disable your account and reset your password. Ask your credit union for further instructions.

How can I avoid getting this virus in the future?
Answer – Most anti-virus programs include signatures that can detect and stop these types of trojans. If your anti-virus program gets outdated or not updated, you will not be protected.
It is important to keep your system updated with the latest Operating System and application patches. Use caution when visiting social network sites, free software sites, and reading emails. Do not click on links within emails or open attachments from unknown sources.