CYBER SECURITY ADVISORY

DATE ISSUED:
12 March 2010

SUBJECT: Information and Recommendations Regarding Unauthorized Wire Transfers Relating to Compromised Cyber Networks

A growing threat of fraudulent wire transfers from local businesses and government entities to overseas locations has raised numerous online banking concerns. The incidents primarily target small to medium sized businesses and government entities and may involve amounts as small as $10,000 US dollars or as much as several million dollars. Unlike the more traditional use of United States-based "money mules" (refers to a person who willingly or unwittingly acts as a go-between during the wire transfer process. Traditional fraud attempts utilize money mules to receive transfers into their bank accounts, withdraw the funds and wire the funds to an overseas location using a service similar to Western Union), these transfers involve larger amounts, and are transferred almost directly overseas through a United States-based account within an international bank owned by an overseas company, or into a local account that immediately transfers the money overseas. Once the money is overseas, it is withdrawn immediately by a "drop"(a person who is paid to withdraw the money or pick up the wire transfer).

The majority of these attacks require the attacker to compromise the target computer, install a keylogger, retrieve the keylogger's information, and force the target user to answer banking security questions. Cyber criminals target small to medium-sized businesses due to the fact that they lack the complex security of a large corporation, but maintain a larger cash balance than most individuals.

A significant part of the growing threat to an online banking customer lies within the Zeus Botnet and malware package. The Zeus Botnet, also referred to as Zbot, is a large but fractured botnet controlled by many independent users. The Zeus software allows its user to create and customize their own malware package, which allows for targeting by user type or geographic areas. The creators of Zeus continue to support their software, releasing new versions and providing a service where Zeus users can check and make sure their own Zeus creation is undetectable by common antivirus products. Thus, each Zeus malware user is able to create a personalized botnet. Computers

infected by the Zeus malware feed banking and online financial information back to the owners of that particular botnet. It should be noted, that the Zeus malware is capable of compromising more than just financial records. As each attacker is capable of modifying Zeus to fit their own needs, Zeus could collect information from social networking websites, company login pages and most websites that use a standard login form or the keylogger function could be used without any additional components.

Many banks currently record the Internet Protocol (IP) address of a computer with access to a particular account and/or leave a "cookie" behind once the user is authenticated. Security questions have become the standard authentication method. Zeus also conducts man-in-the-middle style attacks by adding security questions to banking websites. By capturing the user's login information and the standard responses to security questions, the Zeus botnet owner is then able to login to the financial website and answer these questions, authenticating a second IP address. Other attackers may delete the website cookie, forcing the user to answer these questions a second time, thus providing the required information.

Enterprise Recommendations:

Install a security software suite that includes antivirus, anti-spyware, malware and adware detection, from a reputable vendor. Keep the software up-to-date through an automatic update feature and configure it to perform recurring, automated complete system scans on a routine basis. This will help to protect a computer against known viruses, malware, and adware, but remember many viruses, malware, and adware programs are undetectable by antivirus software.

Routinely install all new software and hardware patches or use the automatic update feature when available. Ensure that all your software, including your operating system and application software such as Microsoft Office, Adobe Flash, Apple QuickTime, Adobe Acrobat, etc., are updated as well and not just the computer's operating system.

Use a dedicated computer for all online transactions and implement white listing methods to prevent the system from going to any site/address that does not have a documented business need. Use a single computer with a static IP address for all online banking transactions. If possible, register this IP address with the financial institution. Actively monitor the computer for viruses and other malware and limit this computer from conducting any other Internet activity, including email.

Educate users on good cyber security practices to include how to avoid having malware installed on a computer and new malware trends such as the development of malvertizing, where malware is hidden in the code of a legitimate website.

Implement block/black lists and enforce them on the network perimeter.

Employ advanced authentication techniques for user logins (two-factor authentication).

Monitor log files, especially proxy server logs, for unauthorized/suspicious internet connections coming to and leaving the network.

Whenever possible, do not use a wireless network for financial transactions. If a wireless network must be used, enforce security measures such as enabling encryption and MAC address filtering, changing the service set identifier (SSID) and turning off SSID broadcasting.

Change the default login names and passwords on routers, firewalls, other network equipment and software.

Consider blocking Internet plug-ins on the computers that access online banking accounts. Disabling Flash, scripts, pop-up windows, etc. can be frustrating for general users but prevent multiple exploits.

Use the on-screen keyboard when possible to circumvent keyloggers.

User Recommendations:

Immediately report any suspicious activity in your accounts. There is a limited recovery window and a rapid response may prevent additional losses.

Install a security software suite that includes antivirus, anti-spyware, malware and adware detection from a reputable vendor. Keep the software up-to-date through an automatic update feature and configure it to perform recurring, automated complete system scans on a routine basis. This will help to protect a computer against known viruses, malware and adware but remember many viruses, malware and adware programs are undetectable by antivirus software.

Routinely install all new software and hardware patches or use the automatic update feature, when available. Ensure that all your software, including your operating system and application software such as Microsoft Office, Adobe Flash, Apple QuickTime, Adobe Acrobat, etc., are updated as well and not just the computer's operating system.

Setup and use a "non-privileged user" account on the computer to prevent unauthorized changes to the computer. Use this non-privileged account for web browsing whenever possible.

Make sure the banking site you are using starts with "https://" instead of "http://". The "s" indicates a secure transaction, using a different method of communication than standard Internet traffic5.

Never use a link to reach your financial institution; emails and search engine links should not be trusted. Type the bank's website address into the Internet browser's address bar every time.

Know what the financial institution's website looks like and what questions are asked to verify your identity. Some attacks, known as man-in-the-middle attacks, will change the login page. These changes allow the attacker to see your answers and to add additional security questions. When you log in the information is transmitted to the attacker and to your financial institution, logging you into your bank's website while also giving your attacker all your account information. A vigilant user can sometimes spot these attacks by noticing slight modifications to the bank's standard page: extra security questions, poor grammar, misspellings, a fuzzy or older logo or a change to the location of each feature.

Be suspicious of emails and text messages purporting to be from your institution or a government agency. Financial institutions should not contact you via email to request you to verify information. If you believe the contact may be legitimate, do not use the link provided in the email, instead type in the link to your financial institution in the Internet browser's address bar.

Restrict online purchases to "one-time credit cards" or "Virtual Account Numbers" to reduce the risk of account numbers being compromised. If you do shop with a regular credit card, use only a single credit card, with a low limit. Choose a credit card with an online purchase protection plan if possible and monitor the activity on that card as often as possible; at least every two or three days.

Avoid using check or debit cards for online transactions.

Always lock your computer when you leave it unattended. Set the computer to automatically lock after a set period of inactivity, e.g. 15 minutes.

Do not allow your computer or web browser to save your login names or passwords.

Use a strong password; at least 10 characters combining upper case and lower case letters, numbers and symbols.

Clear the Internet browser's cache before visiting a financial institution' website.

Never access your financial institution or a privileged/sensitive system from a public computer at a hotel, library or public wireless access point.

Properly log out of all financial institution web sites and close the browser window. imply closing the active window may not be enough.

When you are finished with your computer, turn it off or disconnect it from the Internet by unplugging the modem or Ethernet/DSL cable.

Do not open emails from un-trusted sources or suspicious emails from trusted sources. Be aware "Reading Pane" features, like those within Microsoft Outlook, automatically open the emails they display.

Do not visit un-trusted websites or follow links provided by un-trusted sources.

Do not use the same computer for online transactions that children or "non-savvy" Internet users use for regular Internet access.

Do not use the login or password for your financial institution on any other website or software. Do not write it down. Do change it frequently.
.
Do not post your personal information on the web. Your high school, maiden name, date of birth, first car, first school, youngest sibling' name, mother' full name, father's full name, best friend's

ame, etc. are the answers to many security questions on financial web sites. When you post this information, you are making it easier for criminals to gain access to your financial information.

My account was compromised, what now?

Immediately stop using any computers that may be involved and contact your financial institution to request their help in preventing further loss and to aid in the possible recovery of any money.

Begin a log of your activities, including who you have talked with, what information you have and what mitigation steps you have taken.

Ask your financial institution to report the incident to the State, the Federal Bureau of Investigation or the United States Secret Service.

Confirm that your bank reported the incident and call the appropriate agency yourself to provide additional details.