Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

December 11, 2009

POP-UP ADVERTISEMENTS OFFERING ANTI-VIRUS SOFTWARE POSE THREAT TO INTERNET USERS

An ongoing threat exists for computer users who, while browsing the Internet, began receiving pop-up security warnings that state their computers are infected with numerous viruses.

These pop-ups known as scareware, fake, or rogue anti-virus software look authentic and may even display what appears to be real-time anti-virus scanning of the user's hard drive. The scareware will show a list of reputable software icons; however, the user cannot click a link to go to the actual site to review or see recommendations.

The scareware is intimidating to most users and extremely aggressive in its attempt to lure the user into purchasing the rogue software that will allegedly remove the viruses from their computer. It is possible that these threats are received as a result of clicking on advertisements contained on a website. Cyber criminals use botnets to push the software and use advertisements on websites to deliver it. This is known as malicious advertising or malvertising.

Once the pop-up appears it cannot be easily closed by clicking "close" or the "X" button. If the user clicks on the pop-up to purchase the software, a form is provided that collects payment information and the user is charged for the bogus product. In some instances, whether the user clicks on the pop-up or not, the scareware can install malicious code onto the computer. By running your computer with an account that has rights to install software, this issue is more likely to occur.

Downloading the software could result in viruses, Trojans and/or keyloggers being installed on the user's computer. The repercussions of downloading the malicious software could prove further financial loss to the victim due to computer repair, as well as, cost to the user and/or financial institutions due to identity theft.

The assertive tactics of the scareware has caused significant losses to users. The FBI is aware of an estimated loss to victims in excess of $150 million.

Be cautious — cyber criminals use easy to remember names and associate them with known applications. Beware of pop-ups that are offering a variation of recognized security software. It is recommended that the user research the exact name of the software being offered.

Take precautions to ensure operating systems are updated and security software is current.

If a user receives these anti-virus pop-ups, it is recommended to close the browser or shut the system down. It is suggested that the user run a full, anti-virus scan whenever the computer is turned back on.

If you have experienced the anti-virus pop-ups or a similar scam, please notify the IC3 by filing a complaint at www.IC3.gov.