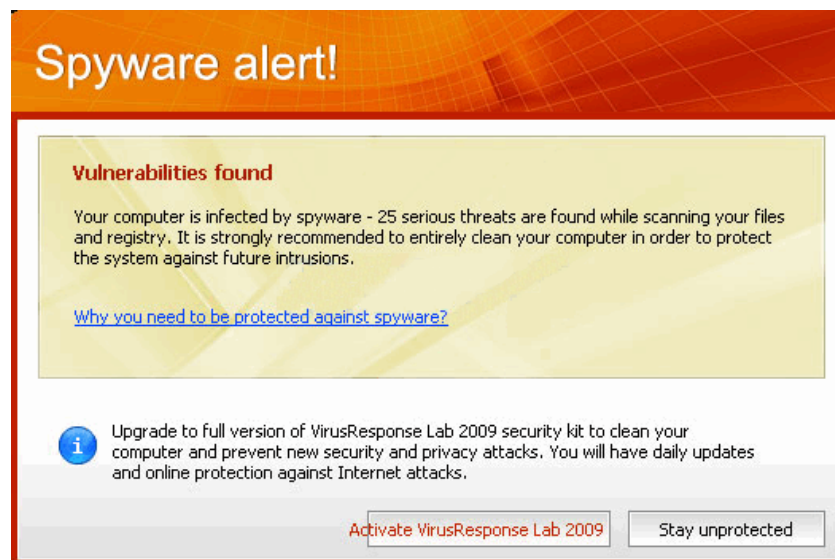


Scareware Advisory

By: John W. Parsell
Date: 10/01/09

LSA.Security has been informed of numerous attempts by hackers to gain control of users' computers by way of bogus popup windows in the web browser. The tactic being used, known as "Scareware," is a variation of a Trojan virus that works by providing a user with false popups upon visiting a website. Clicking these popups can cause a system to become infected, potentially giving the attacker access to sensitive information and/or control of the computer. This attack is only known to affect computers running Windows Operating Systems, and is not specific to any one web browser, meaning users of browsers such as Internet Explorer, Firefox, Flock, Opera, and all others must be aware that their computers are vulnerable to the attack. As with all malicious attacks, a user that thinks that his/her system has been compromised should contact their IT support team immediately.

Scareware popups will commonly inform the user that his/her computer is infected with a virus, spyware, or malware, prompting the user to click inside the dialog box to resolve the problem. In most instances, clicking anywhere within the popup window can compromise the user's computer. Some of these popups will even perform a bogus virus scan on the screen in an attempt to fool the user into believing that his/her computer is infected. Two popups that have been identified as malicious contain references to "Anti Virus 2009," and "Green Anti Virus." In general, any unsolicited popup; security related or otherwise, should be considered a potential threat. These popups contain malicious code that could potentially infect the user's computer, and must not be clicked. Here is an example of a malicious popup:



Source: Image courtesy of <http://www.411-spyware.com/images/Spyware-Alert-popup-VirusTrigger.gif>

As shown in this picture, the dialog boxes ordinarily have no way of being closed without clicking one of the options inside the box, which are commonly "ok" and "cancel." Clicking the cancel (or in this case, the 'Stay unprotected') button is not safe, as it still appears inside of the popup. Some of the popups do contain a "close" feature in the top right corner of the dialog box, such as this one:

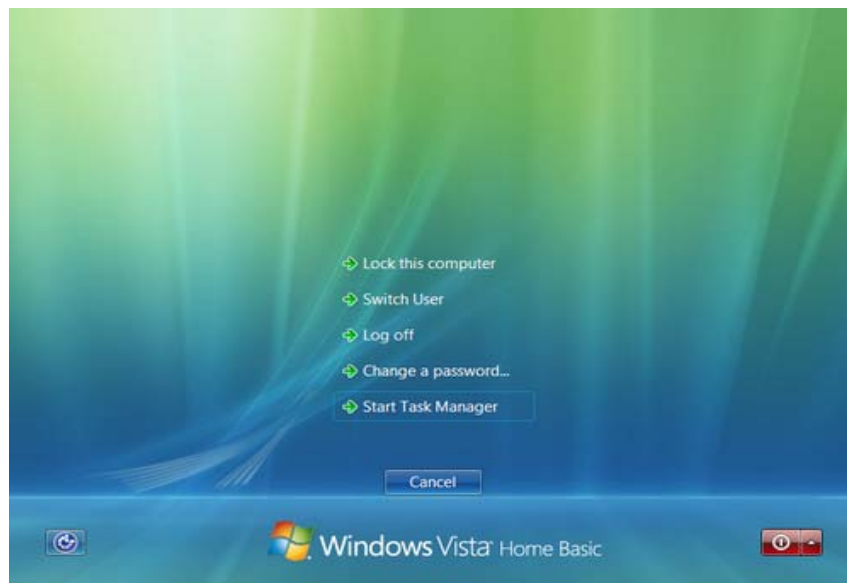


Source: Image courtesy of <http://www.spyware-techie.com/wp-content/uploads/2008/01/homepagecell-popup-warning-message.gif>

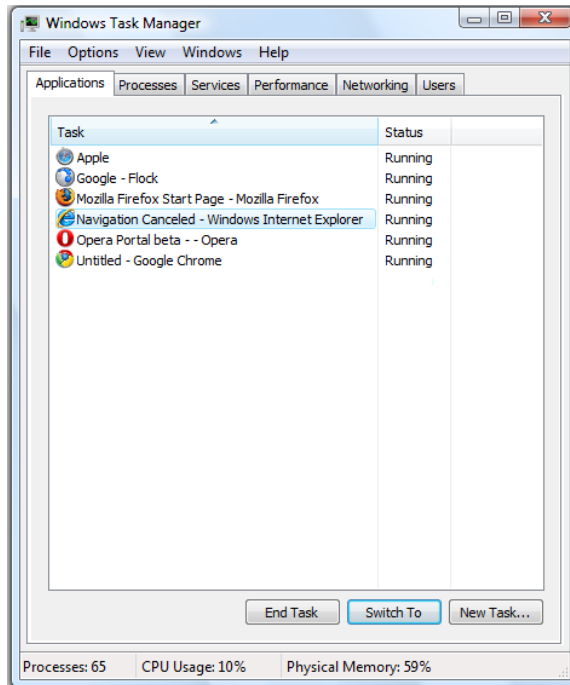
However, using the “close” feature (square button with ‘x’ on it) should not be considered a safe method to eliminating the popup.

Steps for securely closing popups (Windows Vista and Windows 7):

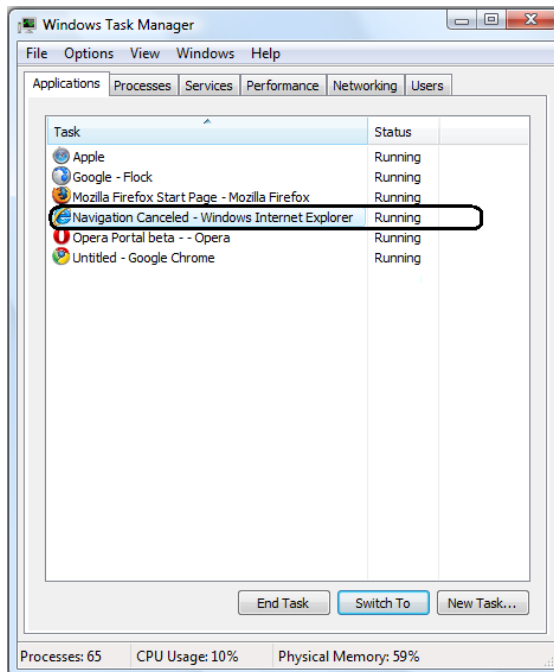
If a user is prompted with a Scareware popup, it can be closed securely by opening the Task Manager, and closing the web browser from the Applications menu. To access the Task Manager from a Windows Vista system, press and hold the Ctrl+Alt+Delete buttons simultaneously. A screen will appear that looks similar to this:



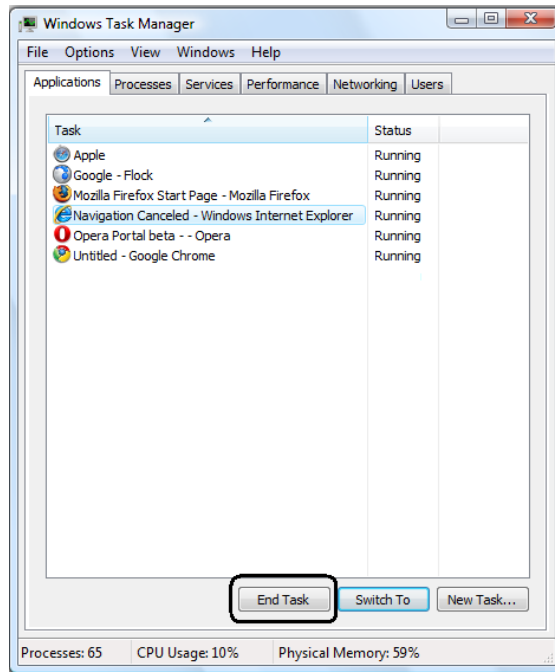
Click on the Start Task Manager button to access Windows Task Manager. A Dialog box should appear in the top left corner, looking similar to this:



First, click on the Applications tab in the Windows Task Manager dialog box (if it is not already selected by default.) Next, highlight your web browser in the task pane by single clicking it (Internet explorer was used in this example; however, the user will be required to select their appropriate browser in the task pane. Popular browsers and their corresponding icons are shown in the picture below:



After your web browser is highlighted, click on the End Task button, located underneath the task pane in the Task Manager dialog box:



Once your web browser no longer appears in the task pane, and has successfully closed, you may close Windows Task Manager. To assure that the system has not been infected, users may choose to perform a virus scan of their system.

Steps for securely closing popups (Windows XP):

For users of the Windows XP operating system, the steps included to close the web browser using the task manager are identical to the steps taken on a Windows Vista system, however there is one minor difference. Upon pressing the Ctrl+Alt+Delete command on the keyboard, users will be greeted with a screen similar to this:

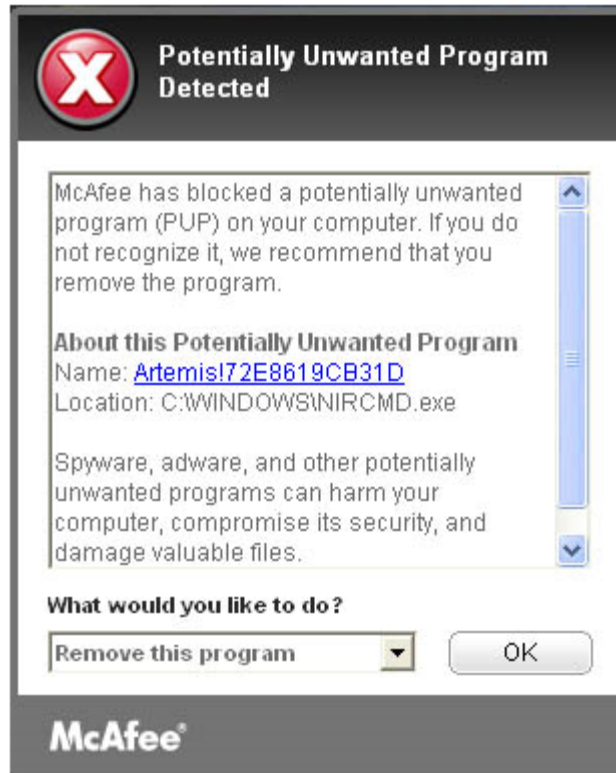


Source: Image courtesy of <http://www.technize.com/wp-content/uploads/2008/06/security1.jpg>

Clicking on the Task Manager button (bottom center) will allow the user to open Windows Task Manager. After doing so, please follow the steps included for ending an Application in Windows Vista (included above.)

Popups from McAfee:

While users must be aware of the proper steps to prevent against a Scareware attack, they must also be familiar with legitimate popups that inform them of malicious software found on their system. The University of Michigan uses McAfee as its Anti-Virus provider, and from time-to-time, the McAfee software may alert a user of a potential threat in their system. While the exact popup from the McAfee software may vary depending on which version the computer is equipped with, an example of a legitimate popup from McAfee is shown here:



Source: Image courtesy of www.bleepingcomputer.com/forums/lofiversion/

As with all vulnerabilities, users should apply their best judgment to any situation. If something looks to be malicious, or if a user is unsure about whether or not an application is safe, they should use caution when making decisions on whether or not to use the application. However, users should be aware that this type of attack is not limited to malicious websites, and that even websites that may have been considered safe in the past can display malicious popups. Also, it is extremely important for a user to keep his/her system up-to-date with the latest AntiVirus updates as well as any patches to help prevent this kind of compromise. Users with questions should contact their computing department or IT support team for any additional information.