GENERAL MALWARE GUIDE

What these Programs do:

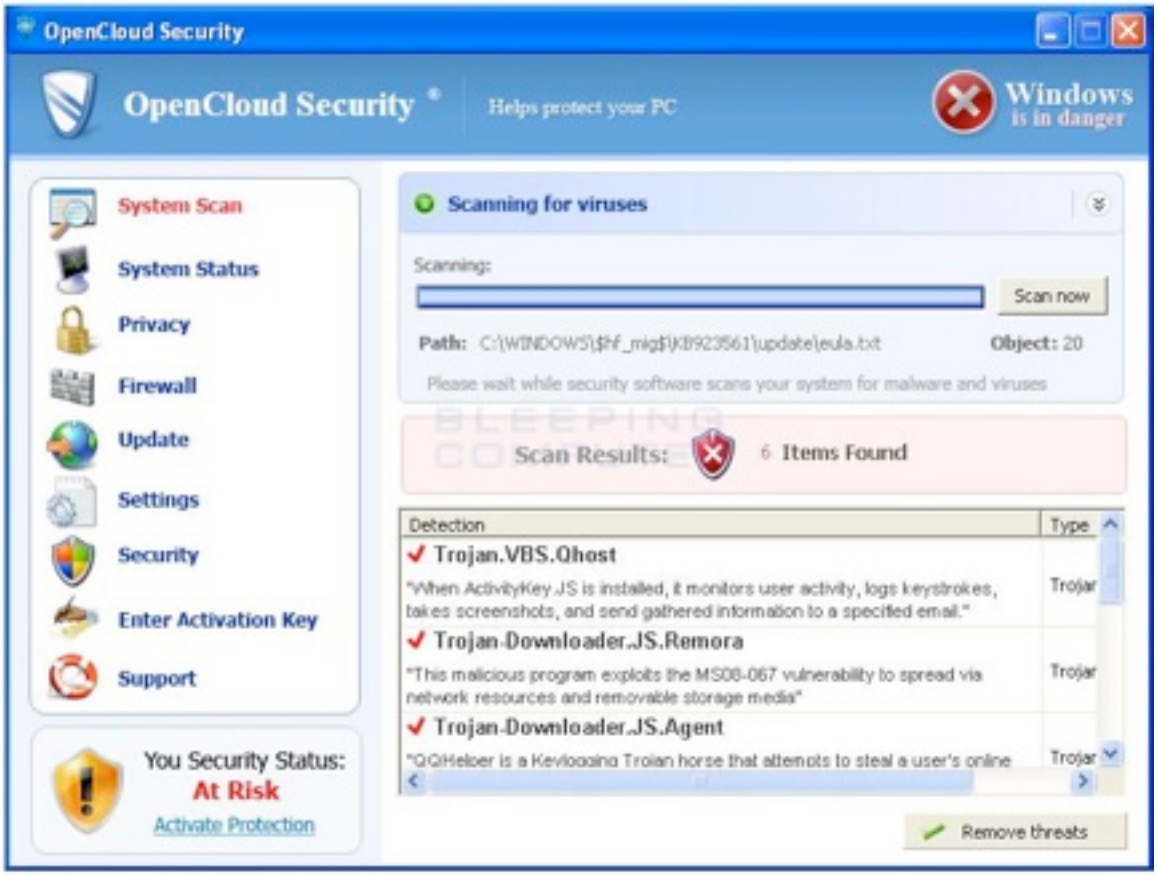
Windows Vista Repair / XP Repair / Windows 7 Repair all belong to a family of rogue anti-spyware programs that are promoted through the use of malware. When installed, these programs will be configured to start automatically when you log into Windows. Once installed, it will also create fake files on your computer that have random filenames. These files are then detected as viruses when the “Repair” program scans your computer. The program though, will state that it will not remove these files unless you first purchase it. This is obviously a scam where the malware / adware is detecting & displaying the files it created in the first place. Therefore, do not act upon any of the scan results this program displays!

While these programs are running you will also see fake security warnings appear on your desktop. These warnings will state that your computer is under attack, that malicious programs are running, or that you are sending personal information to a remote location. Just like the fake scan results, these security warnings are all fake and are only being shown to scare you into purchasing the program (Which is why these programs are also often referred to as “Scareware”)

Without a doubt, this program is a scam and you should not purchase this program regardless of what it may state. If you have already purchased the program, then please contact your credit card company and dispute the charges.

DO NOT SUBMIT YOUR CREDIT CARD INFORMATION!

As seen in the image above, you may receive messages in your Taskbar. These are the same program and should NOT be ignored.



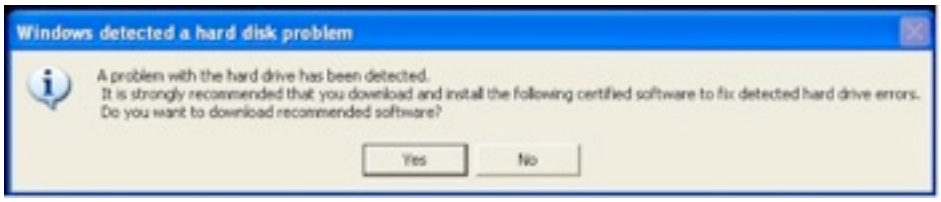
These are representative images and the particular infection you may have could be any number of a similar type program. There are new variants which have appeared recently, but the messages that are displayed will look very similar to these.

Because of the frequency with which these infections are being distributed, it is absolutely imperative that you keep your PC's Antivirus program and Windows Defender up to date with the most recent definitions.

As seen in the image above, you may receive messages in your Taskbar. These are the same program and should NOT be ignored.

Bear in mind ~ once you begin to see these messages, your computer has already been compromised. It is recommended that you do NOT interact with these popups at all, rather:

1. Hit the Control / Shift + Esc keys.
2. This will open your Task Manager.
3. Click on the “Processes” tab.
4. Look for any processes that usually include the name of the program. In this example, it could be something like “AntivirusPC2012.”, “AV12.exe”, “avpc.exe”, etc.
5. Left click on the item to highlight it and then click “Processes in the lower right.
6. You will be asked to confirm your selection ~ click “Yes” or “OK”



A common misconception regarding popups: Whether you click the “Close”, &”No”, “Cancel” buttons or you click the “X” button in the upper right-hand corner ~ the malware either already IS installed or will begin the instant you click anywhere on the popup dialog box. Clicking the “X” does NOT prevent you from being infected.

This type of infection is disguised as a helpful program, but its' only purpose is malicious, hence: Malware. Bear in mind that the root cause of these infections is malware, NOT true viruses. In many cases, the distributed malware will disable your Antivirus and then ALLOW a virus to attack your system.

DO NOT SUBMIT YOUR CREDIT CARD INFORMATION!

- The best course of action is to force a shutdown of your computer by pushing and holding the power button until your computer shuts down.
- If you suspect your computer is infected with one of these programs, bring your computer to a computer professional. We have many tools and utilities at our disposal that are not available commercially.
- Certain information and images courtesy of www.Bleepingcomputer.com.