TIPS TO FIX A ZOMBIE PC

Do you know that your computer might be committing **crime** at the moment? Your computer may become a "*zombie*" if *it is infected with a worm or virus and hijacked by a hacker/cracker*. Here are some tips to see if your computer is infected and remedy the problem.

A **zombie** is a computer infected with a worm or virus and used without your knowledge. The pirate away partially or totally the use of the computer and it so often discreet.

A computer becomes a zombie for several reasons:

- Antivirus inadequately updated.
- A misconfigured firewall or absent.
- An operating system never updated and non-patched.

Only one of these gaps on a computer just for worms like **Bagle / Beagle** or **Gaobot**, and hundreds of variants, "*zombifient*" your computer.
It is estimated that large number of computers in the world, become zombies. A recent publication of the **Symantec Internet Security Threat Report** shows that over a quarter of zombies would residence in the U.S. Your computer may become a "zombie" if it is infected with a worm or virus and hijacked by a hacker. The zombies are not fancy.

A *real zombie market has developed*, exchanges of botnet (*network of thousands of zombies*) has been practiced by pirates and criminal . These groups of zombies and allow the mass mailing of spam, computer attacks of denial of service or the spread of malware. All this being done discreetly without the knowledge of the owners of hijacked computers. The latest date being Waledac botnet and Zeus.

- Hacker identifies an Internet unprotected computers that can easily be infected by a worm. The attacker infects unprotected computers with a worm to make zombies obeying;
- The attacker uses the zombies it comes to infect any type of trigger for attacks on the internet.

The zombies act without the computer owners realize this. They nevertheless remain legally responsible for actions carried out via their connection.

Here are some tips to see if your computer is infected and remedy the problem. How to save your computer

- Install anti-virus and anti spyware software from a trusted source. **Anti-malware** software scans and monitors your computer for known viruses and spyware. If you find something, this software will warn and help you is to take the necessary measures.
- Keep all software up to date regularly install updates for all your software and sign up for automatic updates if possible.
- Use strong passwords and keep them secret. Use our *password-checking* program, the security of your password to identify down.
- Never turn off the firewall. A firewall is a protective barrier between your computer and the **Internet**. If you disable the firewall just for a minute, it increases the risk that your PC is infected with malicious software.
- Take advantage of flash drives with care. By connecting a **flash drive** (memory stick) to an infected computer can take the drive and, in consequence, damage your computer.

Do not be tempted to download malicious software

- Cyber criminals can take your computer into a botnet in the following ways:
- Through the integration of malicious software downloads that you hold for images or movies, or links that you click in **e-mail** or **instant messaging** (IM) messages, or through a social network.
- Or some prompt shows your computer affected by false virus alarms, get to click a button or a link.

This is what you should do

- Keep up your operating system, antivirus and antispyware ;
- Download a free firewall or enable **Windows**;
- Enable the [gs firewall] in your router to prevent intrusions;
- Use a secure browser and follow these recommendations;
- *Disconnect* the computer from the **Internet** when you're not using;

Ask yourself this 100 times

Your antivirus is it really on?

- Is it updated?
- Run an online scans in your entire computer.
- run an online scan.

Your firewall

- Do you have a firewall?
- Is it set correctly?

Your operating system

- Do you have automatic updates for **Windows**?
- Do you secure **Windows** by opting for **Service Packs**?

For your internet browsing

- Do not download any suspicious files and to refuse cookies issues ;
- Equip yourself with an anti-spyware software;