Recovering from a Trojan Horse or Virus

Michael D. Durkota and Will Dormann

It can happen to anyone. Considering the vast number of viruses and Trojan horses traversing the Internet at any given moment, it's amazing it doesn't happen to *everyone*. Hindsight may dictate that you could have done a better job of protecting yourself, but that does little to help you out of your current predicament. Once you know that your machine is infected with a Trojan Horse or virus (or if your machine is exhibiting unexpected behavior and you suspect that something is wrong), what can you do?

If you know what specific malicious program has infected your computer, you can visit one of several anti-virus web sites and download a removal tool. Chances are, however, that you will not be able to identify the specific program. Unfortunately your other choices are limited, but the following steps may help save your computer and your files.

1. Call IT support
If you have an IT support department at your disposal, notify them immediately and follow their instructions.

2. Disconnect your computer from the Internet
Depending on what type of Trojan horse or virus you have, intruders may have access to your personal information and may even be using your computer to attack other computers. You can stop this activity by turning off your Internet connection. The best way to accomplish this is to physically disconnect your cable or phone line, but you can also simply "disable" your network connection.

3. Back up your important files
At this point it is a good idea to take the time to back up your files. If possible, compile all of your photos, documents, Internet favorites, etc., and burn them onto a CD or DVD or save them to some other external storage device. It is vital to note that these files cannot be trusted since they are still potentially infected. (Actually, it's good practice to back up your files on a regular basis so that if they do get infected, you might have an uninfected set you can restore.)

4. Scan your machine
Since your computer (including its operating system) may be infected with a malicious program, it is safest to scan the machine from a live CD (or "rescue" CD) rather than a previously installed antivirus program. Many antivirus products provide this functionality. Another alternative is to use a web-based virus removal service, which some antivirus software vendors offer (try searching on "online virus scan").

The next best action is to install an antivirus program from an uncontaminated source such as a CD-ROM. If you don't have one, there are many to choose from, but all of them should provide the tools you need.

After you install the software, complete a scan of your machine. The initial scan will hopefully identify the malicious program(s). Ideally, the anti-virus program will even offer to remove the malicious files from your computer; follow the advice or instructions you are given.

If the anti-virus software successfully locates and removes the malicious files, be sure to follow the precautionary steps in Step 7 to prevent another infection. In the unfortunate event that the anti-virus software cannot locate or remove the malicious program, you will have to follow Steps 5 and 6.

5. Reinstall your operating system
If the previous step failed to clean your computer, the most effective option is to wipe or format the hard drive and reinstall the operating system. Although this corrective action will also result in the loss of all your programs and files, it is the only way to ensure your computer is free from backdoors and intruder modifications.

Many computer vendors also offer a rescue partition or disc(s) that will do a factory restore of the system. Check your computer's user manual to find out whether one of these is provided and how to run it.

Before conducting the reinstall, make a note of all your programs and settings so that you can return your computer to its original condition.

It is vital that you also reinstall your anti-virus software and apply any patches that may be available. Consult "Before You Connect a New Computer to the Internet" for further assistance.

6. Restore your files
If you made a backup in Step 3, you can now restore your files. Before placing the files back in directories on your computer, you should scan them with your anti-virus software to check them for known viruses.

7. Protect your computer
To prevent future infections, you should take the following precautions:

- Do not open unsolicited attachments in email messages.
- Do not follow unsolicited links.
- Maintain updated anti-virus software.
- Use an Internet firewall.
- Securing your web browser.
- Keep your system patched.

To ensure that you are doing everything possible to protect your computer and your important information, you may also want to read some of the articles in the resources section below.

Resources

Before You Connect a New Computer to the Internet
http://www.us-cert.gov/reading_room/before_you_plug_in.html

Home Network Security
http://www.us-cert.gov/reading_room/home-network-security/

Understanding Firewalls
http://www.us-cert.gov/cas/tips/ST04-004.html

Good Security Habits
http://www.us-cert.gov/cas/tips/ST04-003.html

Continuing Threats to Home Users
http://www.us-cert.gov/cas/alerts/SA04-079A.html

Windows Update
http://www.update.microsoft.com/windowsupdate/v6/thanks.aspx?ln=en&&thankspage=5

Protect Your PC
http://www.microsoft.com/security/default.asp