8.5 Virus Infection and Identification

The harsh reality is that no matter what steps you take to prevent virus infections, there is still a chance your system could be infected with a virus. The next question is, what do you do? Some facets of your response will depend upon the severity of the virus and how far it has spread. However, you need to generally focus on three things:

- Stopping the spread of the virus.
- Removing the virus.
- Finding out how the infection started.

8.5.1 Stopping the Spread of the Virus

In the event of a virus infection, the first priority is to stop the spread of the infection. Stopping the infection will depend on how far the virus has spread. If the virus has only affected one machine, you can simply disconnect that machine from the network. However, it is unlikely that you will detect a virus before it has spread beyond a single machine. Given that fact, you will generally need to follow the steps below:

- If the infection is on a segment of a WAN, disconnect from that WAN connection immediately.
- If the infection is on a subnetwork, immediately disconnect that subnetwork.
- If there are servers with sensitive data that are connected (in any way) to the infected machine (or machines), disconnect those servers. This will prevent loss of sensitive data.
- If there are backup devices connected to the infected machine or machines, disconnect them. This will prevent your backup media from becoming infected.

Obviously, your goal is to avoid getting a virus on your system. However, if this unfortunate event occurs, following these steps can minimize the damage and will also revive your system in a shorter period of time.

8.5.2 Removing the Virus

Once you have isolated the infected machine or machines, the next step is to clean them. If you know the specific virus, then you should be able to remove it by running an antivirus program. If you are not aware, please find virus removal instructions on the Internet. In the highly unlikely event that you cannot remove the virus, then you may have no other choice but to format the machine (or machines) and restore them from backups. However, it must be stressed that such a situation is very unlikely.

If you do successfully remove the virus, you will want to scan the machine thoroughly for any other virus infections before reconnecting it to your network. You should be certain it is completely clean before putting it back online.

8.5.3 Finding how the Infection Started

Once you have contained and removed the virus, the next goal is to see that it does not reappear. This is done by finding out how the virus got onto your system in the first place. To do this, you need to investigate the situation in three ways:

- Talk to users of the infected machines and see if anyone opened any e-mail attachments, downloaded anything, or installed anything. Since these are the three most likely avenues for virus infection, they should be checked first.
- Read any online documentation for that specific virus. It will state the normal method of propagation.
- If neither of those avenues tells you what occurred, check any activity