6.1.1

MALWARE:

Viruses, Worms, Logic Bombs & Trojan Horses

(McAfee VirusScan)

MARCH 2004

Laboratory Overview

Objective

At the end of this lab students will be able to manually detect and remove installed Malware. Students will be able to install and use McAfee VirusScan automatic Malware detection and removal software.

Information for Laboratory

A. Students will utilize Microsoft regedit, to edit the windows registry
B. Students will utilize MacAfee VirusScan 2005 Version to automate scanning and removal of Malware.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Warning

If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor carefully at your own risk.

Execution of this lab will remove any suspect files from previous labs.

Estimated Completion Time

60 Minutes

What is Malware?

"Malware" is the term used to describe any and all malicious (harmful) software, including Viruses, Trojans, and Worms.

What is the difference between them all?

- **Viruses**

  Even though "virus" has become a generic term to refer to all types of computer Malware, it actually only applies to one specific type of malicious code/files. A computer virus does the same thing a biological virus does, for the most part. It infects a "host" (a file, boot sector, etc.) and then looks for ways to spread. The major things setting it apart from other Malware are that it (1) replicates itself and (2) infects other files instead of existing as a standalone file. Viruses can be very harmful, sometimes damaging files, or even erasing them.

- **Worms**

  Worms do not attach themselves to a host program or file the way a virus does; worms reside in active memory and stand alone with no need for a host. A worm does replicate itself like a virus, but it doesn't do so by altering files. Instead, it replicates over computer networks. For example, email worms like Melissa, or Bug Bear replicate over private networks and the Worldwide Web network using email systems. Worms like Code Red replicate over the Web and private networks without using email systems, but other system vulnerabilities.

- **Trojans**

  A Trojan, or Trojan horse program does not replicate itself, and it does not infect other files. A Trojan horse program is a

malicious program that is contained within, or masquerades as, an innocent and useful program. The most widespread type of Trojan program is the type that installs “backdoor” access to a computer, through which a malicious person is allowed to remotely take control of the infected computer. An example of this is the BackOrifice Trojan program. The next most popular type is designed simply to steal passwords, credit card numbers, online banking data, or other personal information and send that information back to the malicious party. Often, a Trojan program arrives, unknown to the victim, along with a screensaver or game. When the screensaver or game is run, it is designed to then install the Trojan program that is included with it. In that kind of scenario, the screensaver or game would be called a “dropper” because it “drops” the Trojan program onto the system.

- **Virus Hoaxes**

  Virus Hoaxes are not just harmless pranks. There are a lot of viruses out there. And then there are some viruses that aren't really out there at all. Hoax virus warning messages are more than mere annoyances. After repeatedly becoming alarmed, only to learn that there was no real virus, computer users may get into the habit of ignoring all virus warning messages, leaving them especially vulnerable to the next real and truly destructive, and virus

- **Other Forms – “Blended threats”**

  Other forms of Malware combine aspects of viruses, worms, and/or Trojans to become what is called "blended threats."

MacAfee VirusScan 2005 Version Anti-virus Software

MacAfee VirusScan is a commercial product capable of automatically cleaning, deleting, or quarantining detected

Malware on the fly. It offers on access and on demand scanning. Most importantly, it has a very large Malware database that is easy to keep up to date with simple web enabled DAT (virus definitions) updates.

PART 1: MANUAL MALWARE REMOVAL

Step 1: Infect your computer

Double click on the file named TEST. This will "infect" or install the test Malware.

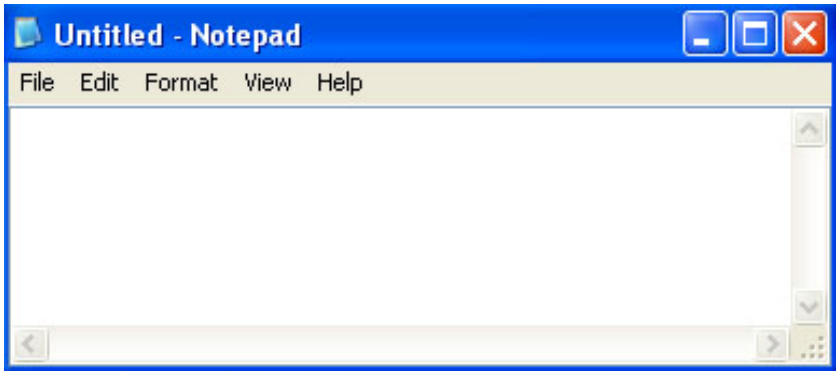
NOTE: This program does NO damage to your computer. This is only to simulate what would happen if real Malware was installed. All effects of this test will be removed by the end of the lab.

Most Malware is loaded and starts with the computer at boot up, and continues to run until the computer is shut off, or the process is manually stopped.

TEST simulates Malware by executing notepad.exe at boot up.

Step 2: Reboot

Once you have infected your computer with the TEST Malware program, reboot your computer. Notice that at startup, notepad.exe starts automatically, and will stay running until you close it. Leave it open for now.



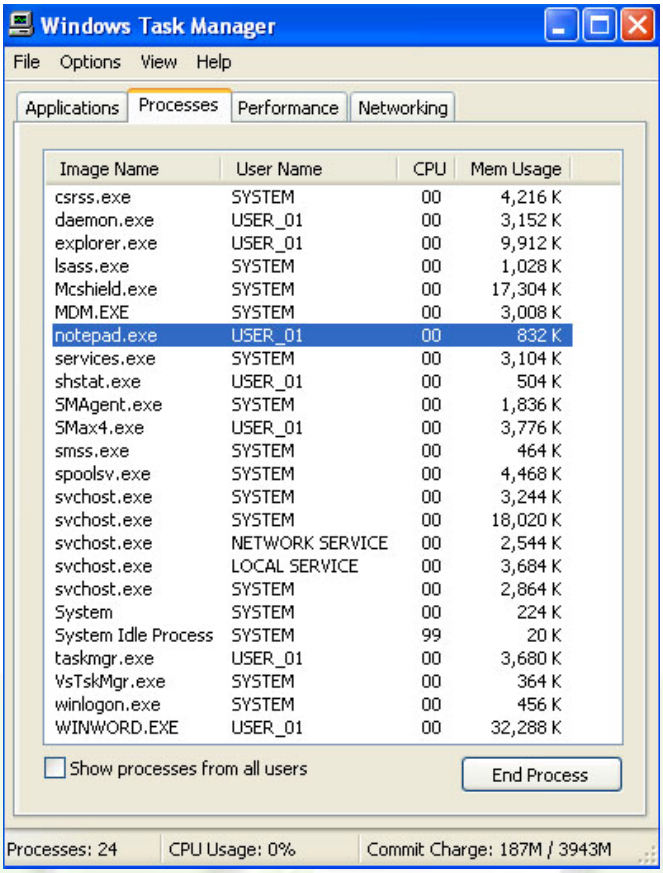
Note: Notepad.exe is a text editor that comes with Windows, and is harmless. Real world Malware programs that execute and stay running can cause serious problems.

Remember for testing purposes in this lab, that this instance of notepad running, is to simulating Malware, and could actually be a Virus or Trojan running that was deleting your data, spreading itself, or sending your personal information out on to the Internet. Most Malware does not make itself so obvious by opening a window that you can see. Usually, Malware programs run hidden in the background, and try to be invisible to the user.

Step 3: Detecting installed Malware

From your Windows computer, press Alt+Ctrl+Del, and then click on Task manager. Click on the second tab, Processes. This is a list of processes that are currently running on your computer. If any programs are running, Malware or not, it is on this list.

It is a good idea to take a snapshot of your process list after a clean install of Windows. This way you can compare it to your system at a later date, and know what should and should not be running.



In the process list, notice that notepad.exe is listed. Click on the line for notepad, it should then be highlighted like above, then click the box End Process. This will end the notepad.exe process, stopping and closing the notepad program.

Step 4: Reboot

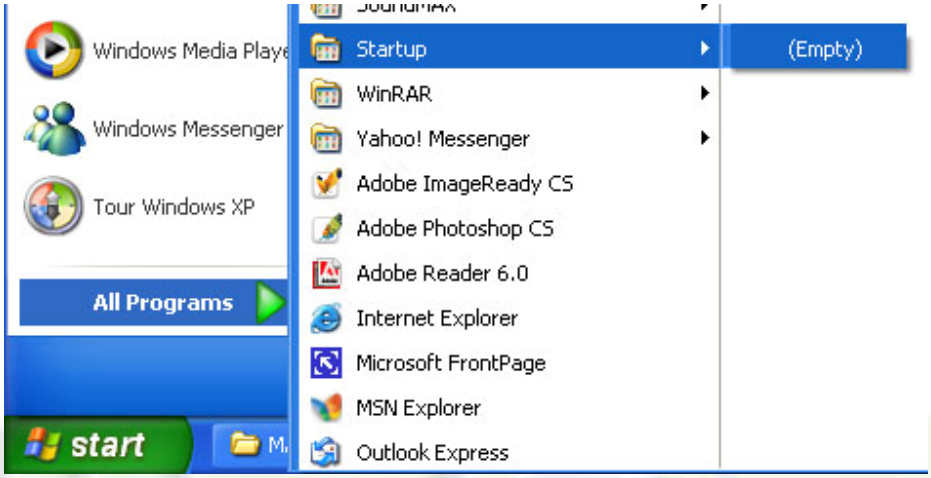
Now that you ended the notepad process, and stopped the program, reboot the computer.

Did notepad open at boot up again?

Step 5: Removing the Malware from startup

We saw in the previous step, that ending a process only lasts for that session, and once the computer is rebooted, the process is automatically restarted. Windows has several different ways of automatically launching applications upon

startup. The first and most obvious is the startup folder. Click START, All Programs, then Startup. Anything that is in this folder will automatically launch when windows first boots up. Since notepad.exe is not in the startup folder, we must look to the other possible locations.



Step 6: Looking in the Windows Registry for Autostart Keys

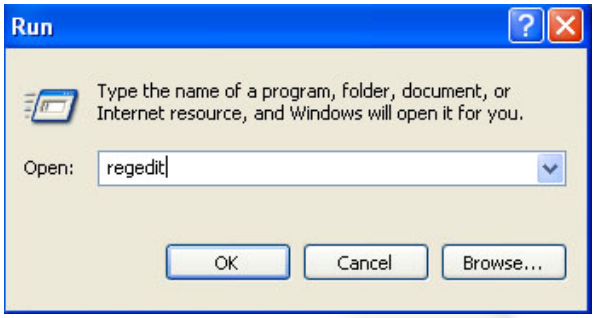
Software can also be launched from the windows registry. There are specific registry keys designed to launch applications at startup. The \HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\CurrentVersion key contains 3-6 folders that are a part of the Windows Autostart registries.

"Run"
"RunOnce"
"RunOnce\Setup"
"RunOnceEx"
"RunServices"
"RunServicesOnce"

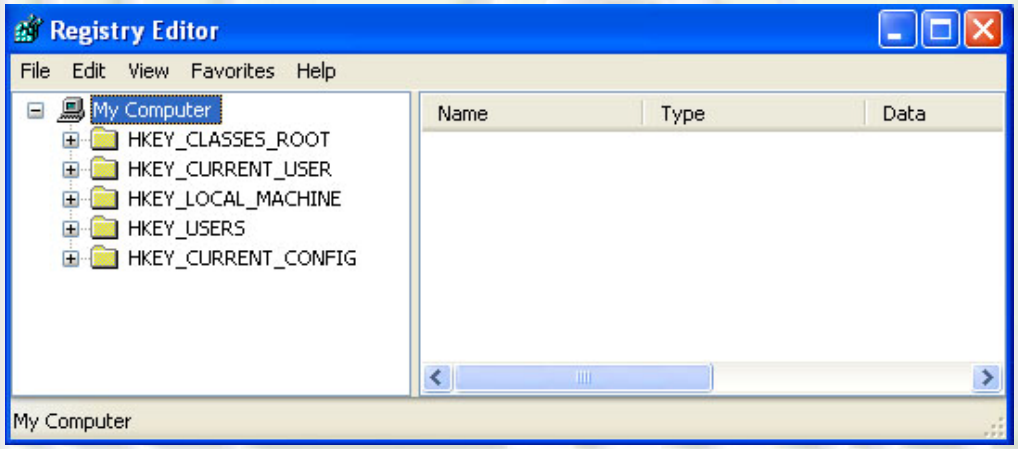
The most commonly used is the Run key. This registry key is commonly used, because it autostarts applications for the local machine, and effects any and all users of the machine.

Warning: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Please pay close attention, and follow the specific instructions.

Click START, RUN, and type regedit in the Open: box, then click OK



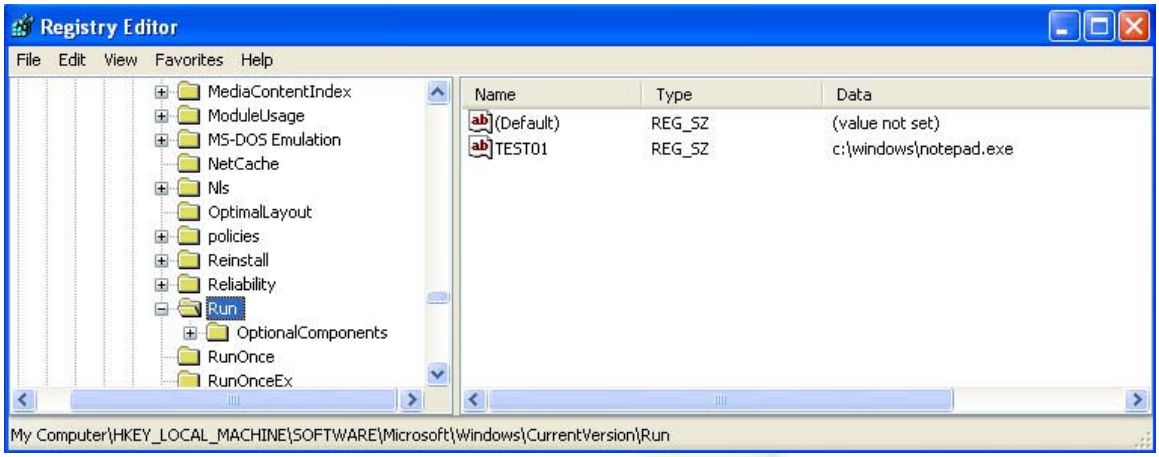
When regedit is opened, it should look like this



Notice the Plus and Minus sign next to the HKEY_. If your nodes are expanded, click on all the minus signs until you get to this stage.

Since we now know where the autostart registry entries are, let's navigate to the \HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\CurrentVersion\Run Key.
Double click on first level \HKEY_LOCAL_MACHINE, and expand that node. Scroll down the list to the second level, the

SOFTWARE Key, and expand that node. Again, scroll down to now the third level, the Microsoft Key, and expand that node. Continue to the Windows\CurrentVersion\Run Key.



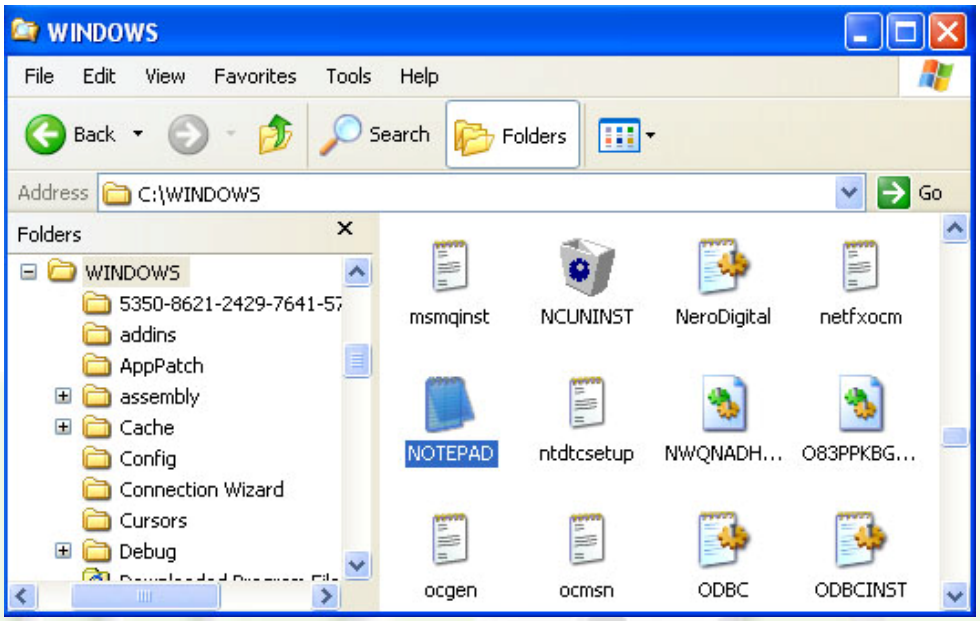
You will notice that when you find the Run key, there is an entry named TEST01. Depending on your computer, and installed software, there may be several other entries listed. TEST01 as listed has an entry for c:\windows\notepad.exe. Make a note of this directory path for the next step. This is the autostart entry that is starting notepad.exe every time the computer boots up. To delete this auto starting entry, simply click on TEST01 and press Delete on the keyboard. You will be prompted to verify you're sure, Click yes.

The entry TEST01 should now be gone.

Step 7: Deleting the Malware program

From your notes in the previous step, using Windows explorer, navigate to the listed directory, and locate the file.

C:\Windows\notepad.exe



If this was a real Malware program, we would want to delete the file. Since notepad.exe is a commonly used windows component, and only used for an example, we will NOT delete it, but stop here.

PART TWO: AUTOMATIC MALWARE REMOVAL

Step 1: Installing MacAfee VirusScan 2005 Version

McAfee no longer installs via a downloaded file, but rather installs directly over the Internet. To install, use Internet Explorer and go to,

www.mcafee.com

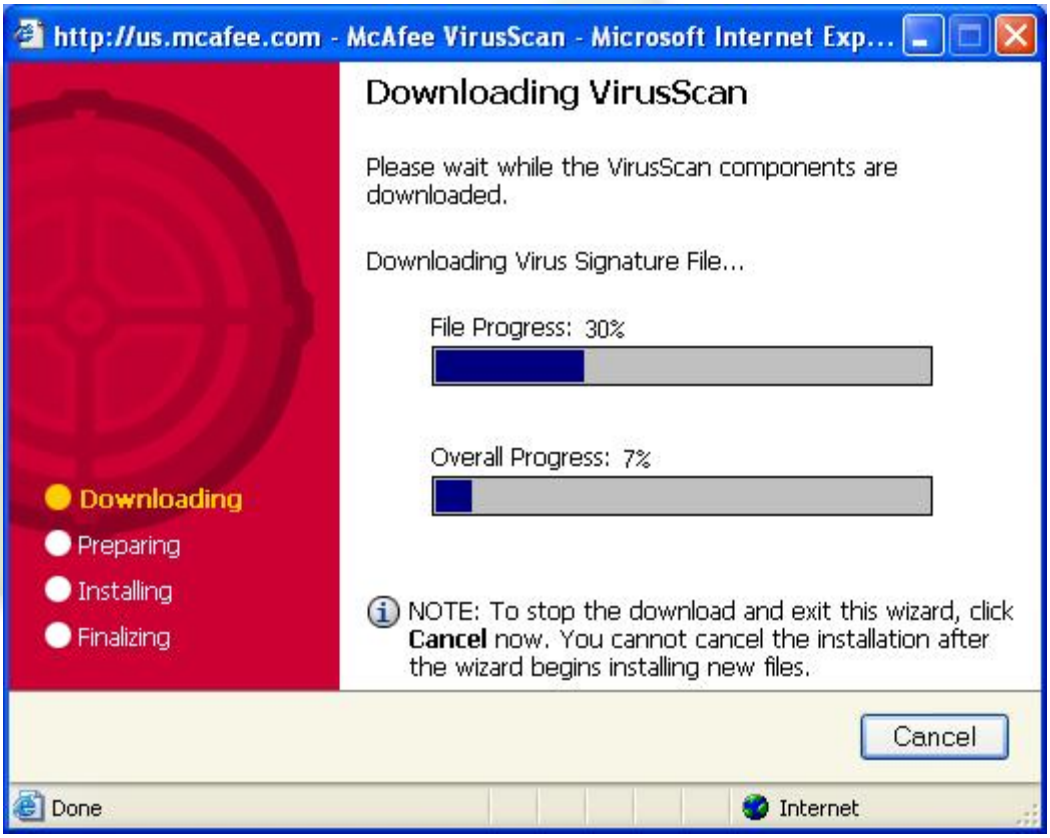
At the home page, navigate to Home & Home Office.

From the Home & Home Office page, dropdown the downloads menu to Free Trial Software. Select the McAfee VirusScan 15-Day Free Trial and add to cart. You can say No Thanks to the upgrade, which takes you to the account page. Fill out the account page and agree to the license agreement.

You should arrive to a page indicating a successful order. Prior to attempting to download, go to your email and activate your McAfee account via the link in the email McAfee has sent you. Back at McAfee, proceed to My Account, and at the account page, Download/Install Update. Agree with the license agreement.

McAfee VirusScan will download and install. You may need to install an Active X control from McAfee.

You may also be required to allow popups. The ensuing download will take several minutes.



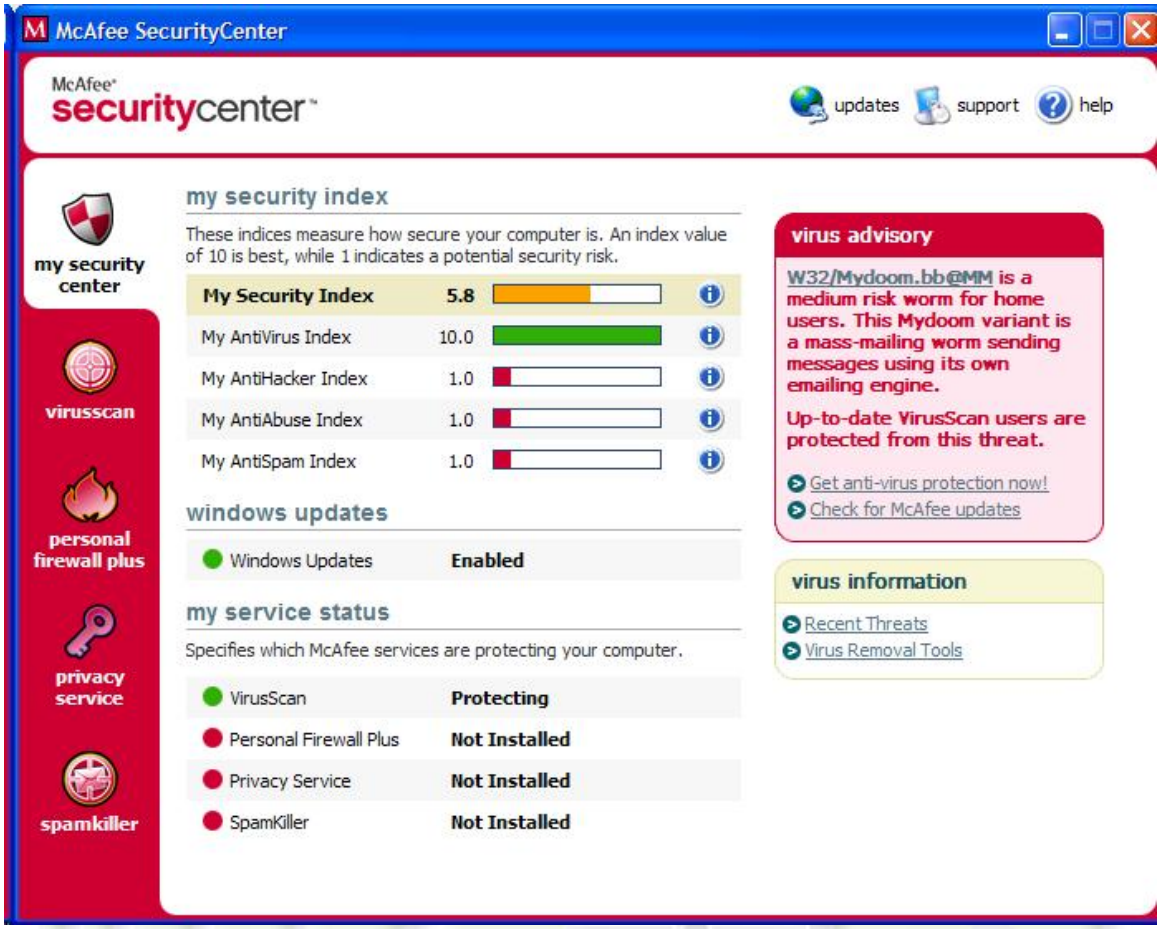
After downloading, click next for preparing installation.

The actual installation proceeds quickly. There is no need to participate in Virus Map Reporting. Simply follow the prompts and finalize. After McAfee has installed, select McAfee as your Security Center.

Click next and finish. McAfee will execute the update engine and will display an alert based on recent malware risks. McAfee will also start the ActiveShield which protects your computer from viruses.

Step 2: Using McAfee Security Center

Activate the McAfee Security Center via the system tray, or the desktop icon. By default, automatic Windows updates are enabled. Keeping antivirus software up to date has become critical. In recent years the amount of malware has increased dramatically while at the same time the response time necessary to mitigate damaging effects has been significantly reduced. You can always check for updates manually through the updates tool button on the upper right. You can also change your update options.

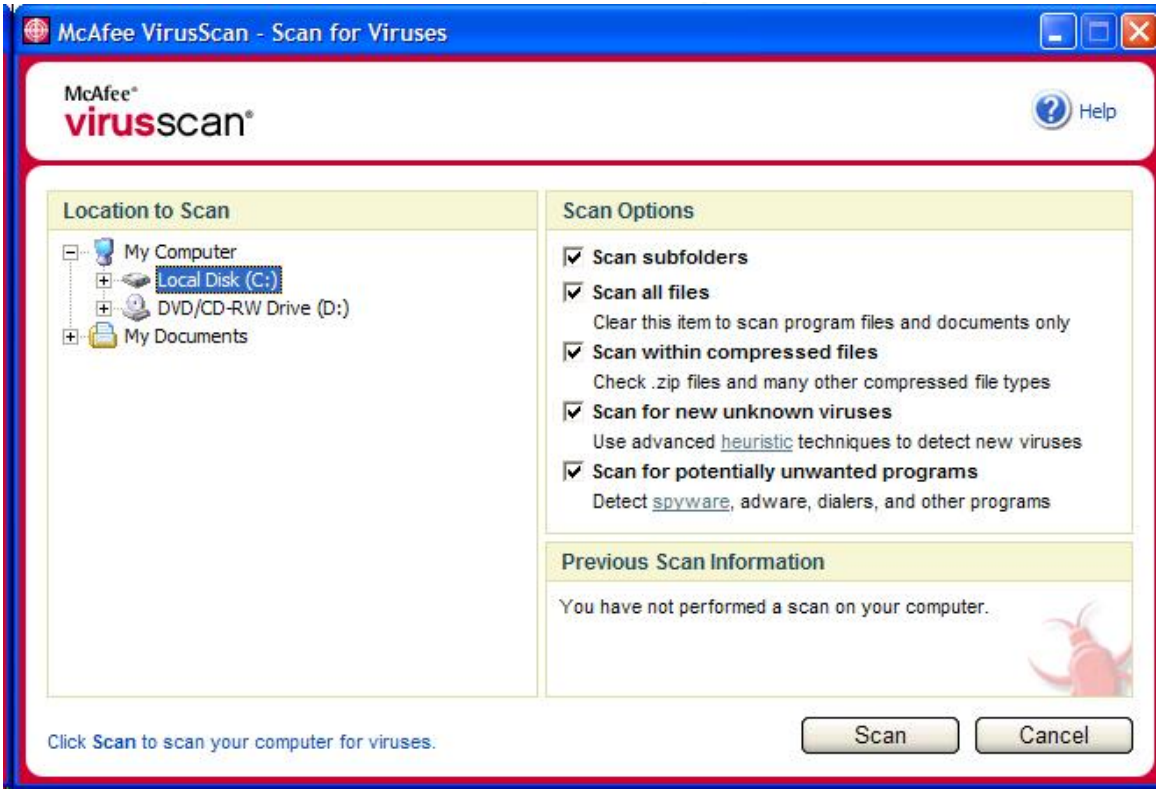


Check now for updates.

View the additional information available at the McAfee Security Center. McAfee offers a family of security tools, not just antivirus.

Step 3: Using McAfee VirusScan to Scan your System

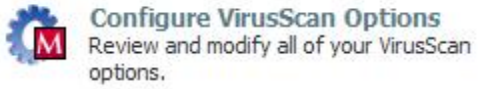
Since there could possibly be a virus somewhere on your hard drive that has not yet been accessed or executed, a full system scan is required. You can activate the McAfee VirusScan dialog box from the Security Center, the VirusScan desktop icon, or the Start menu.



Simply select the drive and scan. Of course this may take considerable time, and results of the scan will vary.

Step 4: Configure McAfee VirusScan Options

From the Security Center, select virusscan on the left, and then Configure VirusScan Options.



Explore ActiveShield and Scheduled Scan options.

Part 3: Analysis

1) For which applications is automatic malware detection and removal best suited?

2) After working with these utilities, what about Malware do you feel you should study further? Why?

3) Why should you enable on access scanning?

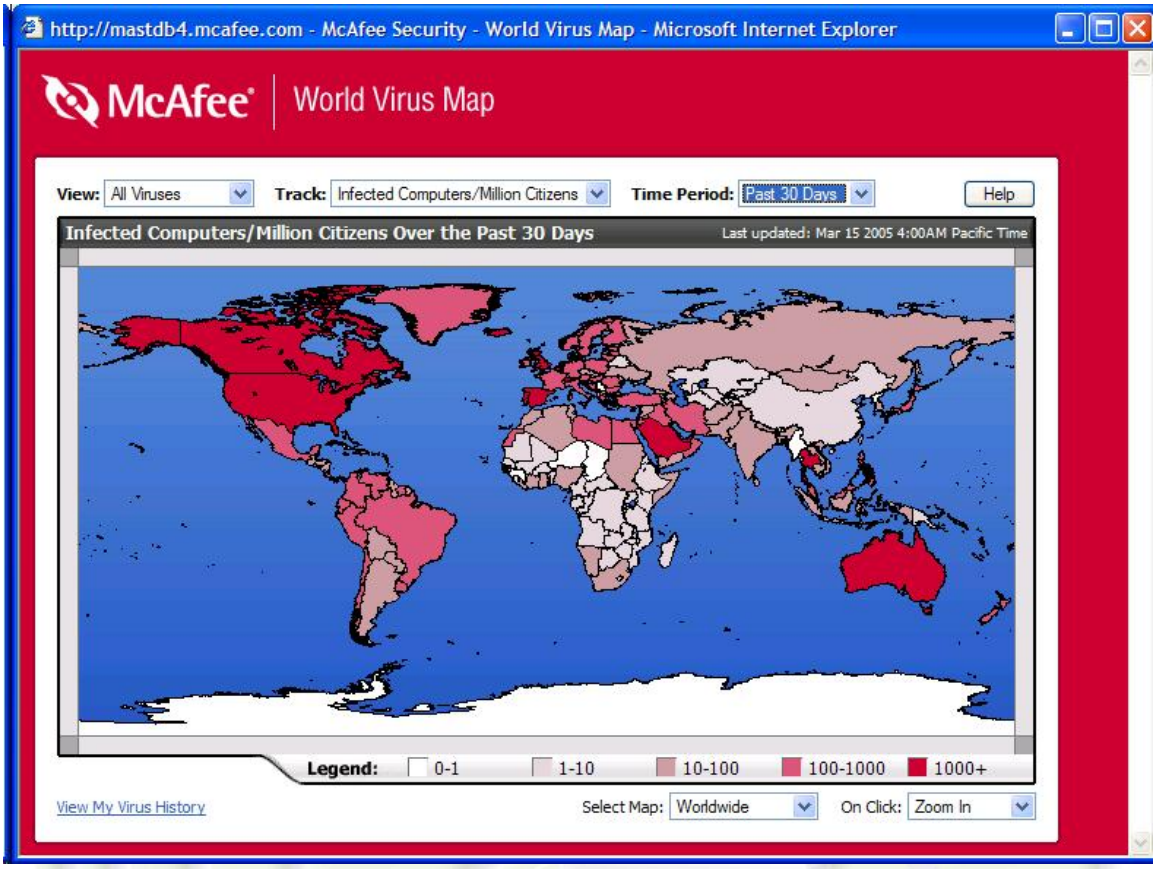
4) Why should you do a full system scan?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Explore View the World Virus Map from the Security Center, virusscan tab.



Appendix:

This lab was developed using McAfee VirusScan 2005 Version, which can be obtained from:

www.mcafee.com

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).