13.6.9 Malware Protection Facts

You should protect all systems with malware protection software in order to help prevent infections and remediate systems if an infection occurs.

This lesson covers the following topics:

- Malware
- Malware symptoms
- Malware infection remediation

Malware

Malware is a type of software designed to take over or damage a computer, without the user's knowledge or approval. Be aware of the following when protecting against malware:

- Most vendors provide products that protect against a wide range of malware including viruses, spyware, adware, and even spam.
- You can install anti-malware software on an individual host system or on a network server to scan attachments and files before they reach the end computer.
- Most anti-malware software that protects a single host uses a signature-based scanning system.
  - Signature files (also called definition files) identify specific known threats. During a system scan, the anti-malware engine runs and compares files on your computer against the signature files.
  - Anti-malware software that uses signatures can detect only threats that have been identified by an associated signature file. Malicious software that does not have a matching signature file will not be detected. The system is not protected against these files.
  - It is important to keep the signature files up to date. If possible, download new signature files daily. Most anti-malware software will check for updates automatically on a schedule.
  - It is important to keep the scanning engine software updated to add new features and fix bugs in the scanning software.

In addition to using scanning software, you should also do the following:

- Keep your operating system and browser up to date. Make sure to apply security-related hotfixes as they are released.
- Implement software policies that prevent downloading software from the internet.
- Scan all files before copying them to your computer or running them.
- In highly-secure areas, remove any removable drives (such as recordable optical drives and USB drives) to prevent unauthorized software from entering a system.
- Show full file extensions on all files. Viruses, worms, and Trojans often make use of double file extensions to change the qualities of files that are normally deemed harmless. For example, adding the extension .txt.exe to a file will make the file appear as a text file in an attachment, when in reality it is an executable.
- Use Security and Maintenance, in Control Panel to check the current security status of your computer. Security and Maintenance shows if you have antivirus, firewall, and automatic updates running.
- Train users about the dangers of downloading software and the importance of anti-malware protections. Teach users to scan files before running them, and to make sure they keep the virus protection definition files up to date.

Malware Symptoms

If you suspect that your system is infected with malware, keep the following in mind:

- Common symptoms of malware on your system include:
  - The browser home page or default search page has changed.
  - Excessive pop-ups or strange messages are displayed.
  - Firewall alerts about programs trying to access the internet.
  - System errors about corrupt or missing files are displayed.
  - File extension associations have changed to open files with a different program.
  - There are files that disappear, are renamed, or are corrupt.
  - New icons appear on the desktop or taskbar, or new toolbars are displayed in the browser.
  - The firewall or antivirus software is turned off, or you can't run antivirus scans.
  - The system won't boot.
  - The system runs very slowly.
  - Unusual applications or services are running.
- Some malicious software can hide themselves such that there might not be any obvious signs of their presence. Other symptoms of an infection include:
  - Slow internet access.

  - Excessive network traffic, or traffic during times when no activity should be occurring.
  - Excessive CPU or disk activity.
  - Low system memory.
  - An unusually high volume of outgoing email, or email sent during off hours.
- Regular system scans can detect and fix many problems.
  - Most software lets you schedule complete system scans, such as daily or weekly.
  - If you suspect a problem, initiate a full system scan immediately.

Malware Infection Remediation

Remediation is the process of correcting any problems that are found. Most antivirus software remediates problems automatically or semi-automatically (i.e. you are prompted to identify the action to take). Possible actions in response to problems are:

- Repair the infection. This may be possible for true viruses that have attached themselves to valid files. During the repair, the virus is removed and the file is placed back in its original state (if possible). Configuration changes made by the infection may also need to be repaired. For example, if the virus changed the default browser home page or search page, you may need to manually reset them using Internet Options, in Control Panel.
- Quarantine the file. This moves the infected file to a secure folder where it cannot be opened or run normally. You might quarantine an infected file that cannot be repaired to see if another tool or utility might be able to recover the file at another time.
- Delete the file. You should delete malicious files such as worms, Trojan horse programs, spyware, or adware programs. In addition, you should periodically review the quarantine folder and delete any files you do not want to recover.

If a scan reports a serious problem, disconnect your computer from the network. This prevents your computer from infecting other computers until the problem is corrected.

Some malicious software warnings, such as those seen in pop-ups or received through email, are hoax viruses. A hoax virus instructs you to take an action to protect your system, when in fact that action will cause harm. Two common hoaxes are:

- Instructing you to delete a file that is reported as a virus. The file is actually an important system file that will lead to instability or the inability to boot your computer.
- Instructing you to download and run a program to see if your system is compromised or to add protection to your system. The file you download is the malicious software.

Before taking any actions based on notices or emails, search the internet for a list of virus hoaxes and compare your notice to known hoaxes.

A suggested procedure for remediating a system with a malware infection is as follows:

1. Identify the symptoms of the infection.
2. Quarantine the infected system.
3. Disable System Restore in Windows. This prevents the infection from being included in a restore point.
4. Update the anti-malware definitions.
5. Scan for and remove the malware.

   Some malware cannot be removed because it is running. If possible, stop its process from running, then try to remove it. If you are unable to stop the malware's process, try booting into Safe Mode and then run the scanning software to locate and remove the malware.

6. If necessary, schedule future anti-malware scans and configure the system to automatically check for signature file updates.
7. Install any operating system updates.
8. Re-enable System Restore and create a new restore point.
9. Educate the end user to prevent future infections.

Some malware infections could require that you reinstall applications or features, restore files from a backup, or even restore the entire operating system from scratch. If the infection has damaged or corrupted system files, you might be able to repair the infected files using the **sfc.exe** command. Before running sfc, be sure to first remove the malware that caused the damage (or it might re-introduce the problem later). You might need to boot into Safe Mode in order to check system file integrity and repair any problems found.

Some malware can corrupt the boot block on the hard disk preventing the system from starting. To repair this problem, try performing an automatic repair. Use **fixmbr** or **fixboot** in the Recovery Console to try to repair the damage. Alternatively, if your organization uses imaging solutions, you can quickly re-image an infected machine. Re-imaging is often faster and more effective than malware removal and cleanup.