COURSE TECHNOLOGY
CENGAGE Learning™

# Security Awareness
# Fourth Edition

*Chapter 3*
*Computer Security*

# Objectives

After completing this chapter, you should be able to do the following:

- List and describe the different types of attacks on computers
- Explain how to manage patches
- Describe how to install and use antivirus software
- Explain User Account Control
- Describe how to recover from an attack

# Introduction

- Protecting personal computers is challenging
- Many different types of attacks exist today
  - Attackers are constantly modifying attacks and creating new ones
- No single defensive program exists
  - Several different defenses must be in place

# Attacks Using Malware

- Malware
  - Software that enters a computer system without the owner's knowledge or consent
  - Performs unwanted and usually harmful action
- Malware objectives
  - Rapidly spread its infection
  - Conceal its purpose
  - Make profit for its creators

# Malware that Spreads

- Viruses
  - Malicious computer code that reproduces on a single computer
- Methods of spreading virus
  - Virus appends itself to a file
  - Virus changes the beginning of the file
    - Adds jump instruction pointing to the virus
  - Swiss cheese infection
    - Injects portions of code throughout program's executable code

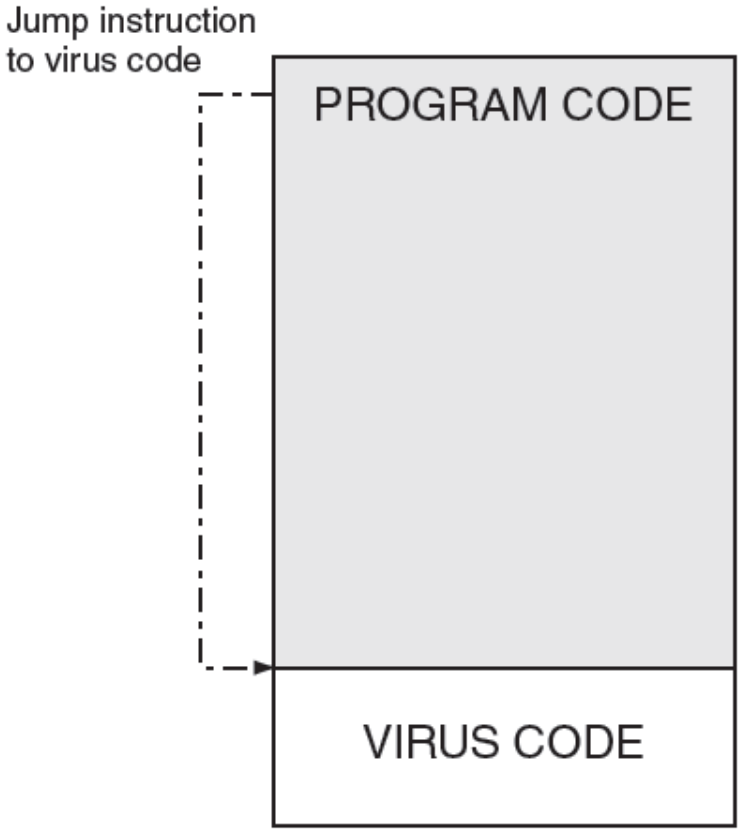


Figure 3-1 Appender infection



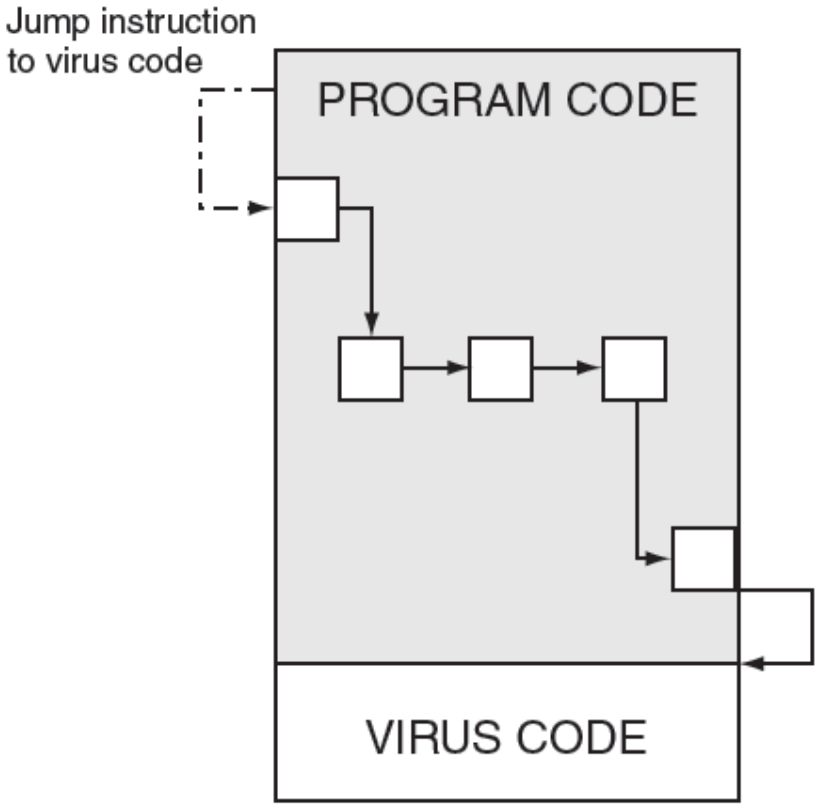


Figure 3-2 Swiss cheese infection

# Malware that Spreads (cont'd.)

- Virus actions
  - Causing computer to crash repeatedly
  - Displaying an annoying message
  - Erasing files from hard drive
  - Making copies of itself to consume all space on the hard drive
  - Turning off security settings
  - Reformatting the hard drive

# Malware that Spreads (cont'd.)

- Virus can only replicate on host computer
  - Cannot spread between computers without user action
- Types of viruses
  - Program virus
    - Infects program executable files
  - Macro virus
    - Stored within a user document

# Malware that Spreads (cont'd.)

- Worm
  - Malicious program designed to take advantage of a vulnerability in an application or operating system
  - Searches for another computer with same vulnerability
  - Sends copies of itself over the network
- Worm actions
  - Consume network resources
  - Allow computer to be controlled remotely
  - Delete files

| Action | Virus | Worm |
|---|---|---|
| How does it spread to other computers? | Because viruses are attached to files, they are spread by a user transferring those programs to other devices. | Worms use a network to travel from one computer to another. |
| How does it infect? | Viruses insert their code into a file. | Worms exploit vulnerabilities in an application or operating system. |
| Does there need to be user action? | Yes | No |
| Can it be remote controlled? | No | Yes |

Table 3-1 Difference between viruses and worms

# Malware that Conceals

- Types of concealing malware
  - Trojan
  - Rootkit
  - Backdoor
  - Arbitrary code execution
- Trojan
  - Executable program containing hidden malware code
  - Program advertised as performing one activity but actually does something else

# Malware that Conceals (cont'd.)

- Trojan may be installed on user's system with user's approval
- Trojans typically do not replicate to same computer or another computer
- Rootkit
  - Set of software tools used by an attacker
  - Conceals presence of other malicious software
  - Actions
    - Deleting logs
    - Changing operating system to ignore malicious activity

# Malware that Conceals (cont'd.)

- Backdoor
  - Software code that gives access to program or service
    - Circumvents normal security protections
- Often created by software developers during development
  - Intent is to remove backdoor
  - Sometimes they are not removed in released program
- Malware from attackers can install a backdoor on a computer

# Malware that Conceals (cont'd.)

- Keylogger
  - Hardware or software that captures keystrokes
  - Information can be retrieved by an attacker
- Hardware keylogger
  - Installed between computer keyboard and USB port
- Software keylogger
  - Hides itself from detection by the user

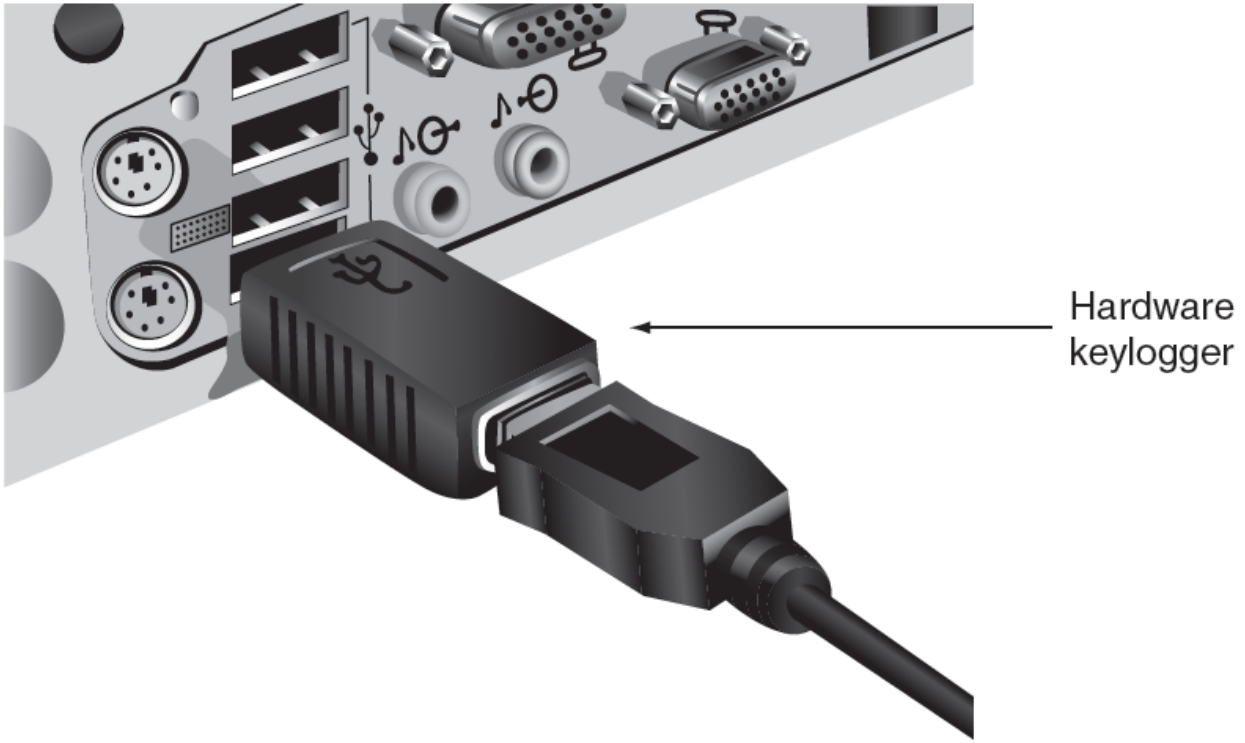


Figure 3-3 Hardware keylogger

# Malware that Conceals (cont'd.)

- Arbitrary code execution
  - Attacker uses buffer overflow attack to gain control of victim's computer
- Buffer
  - Storage area on computer that contains "return address" for computer processor
- Buffer overflow attack
  - Attacker substitutes own return address in the buffer
    - Leads to malware code

# Malware that Profits

- Attacker takes control of victim's computer for extended time period
- Zombie
  - Infected ''robot'' computer
- Botnet
  - Hundreds, thousands, or tens of thousands of zombies
- Bot herder (attacker) uses controls zombies using HTTP commands
- Botnets can remain active for years

| Type of Attack | Description |
|---|---|
| Spamming | A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam. Some botnets can also harvest e-mail addresses. |
| Spreading malware | Botnets can be used to spread malware and create new zombies and botnets. Zombies have the ability to download and execute a file sent by the attacker. |
| Manipulating online polls | Because each zombie has a unique Internet Protocol (IP) address, each "vote" by a zombie will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way. |
| Denying services | Botnets can flood a Web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests. |

Table 3-2 Uses of botnets

# Malware that Profits (cont'd.)

- Botnets often used to send spam e-mail
- Spyware
  - Software that spies on the user without user's consent
- Spyware actions
  - Control use of system resources
  - Collect personal information
  - Impact user experience, privacy, or system security

| Technology | Description | Impact |
|---|---|---|
| Automatic download software | Used to download and install software without the user's interaction | Can be used to install unauthorized applications |
| Passive tracking technologies | Used to gather information about user activities without installing any software | Can collect private information such as Web sites a user has visited |
| System modifying software | Modifies or changes user configurations, such as the Web browser home page or search page, default media player, or lower-level system functions | Changes configurations to settings that the user did not approve |
| Tracking software | Used to monitor user behavior or gather information about the user, sometimes, including personally identifiable or other sensitive information | Can collect personal information that can be shared widely or stolen, resulting in fraud or identity theft |

Table 3-3 Technologies used by spyware

# Malware that Profits (cont'd.)

- Spyware's negative effects on an infected computer
  - Slow system performance
  - Create system instability
  - Add browser toolbars or menus
  - Add shortcuts
  - Hijack a home page
  - Increase pop-ups

# Malware that Profits (cont'd.)

- Adware
  - Software program that delivers advertising content:
    - In an unexpected and unwanted manner
- Adware actions
  - Display pop-up ads and banners
  - Open Web browsers at random intervals
  - May display objectionable content
  - May interfere with user productivity
  - May track and monitor user actions

# Malware that Profits (cont'd.)

- Scareware
  - Software that displays a fictitious warning
  - Tries to impel user to take action
  - Uses legitimate trademarks or icons
  - Pretends to perform a security scan and find serious problems
  - Offers purchase of full version of software to fix problems
  - Victim provides credit card number to attacker
    - Attacker uses number to make fraudulent purchases

# Computer Defenses

- Defenses a user should implement
  - Managing patches
  - Installing antivirus software
  - Configuring personal firewalls
  - Using User Account Control
  - Protecting against theft
  - Creating data backups
  - Knowing steps for recovering from an attack

# Managing Patches

- Patch
  - Software security update intended to cover vulnerabilities discovered after the program was released
- Service pack
  - Software package of cumulative security updates and features
- Modern operating systems can perform automatic updates

# Managing Patches (cont'd.)

- Configuration options for updates
  - Install updates automatically
  - Download updates and user chooses whether to install
  - Check for updates and user chooses whether to download and install
  - Never check for updates
- Automatic operating system updates may include updates from other software vendors

# Installing Antivirus Software

- Antivirus software
  - Scans a computer's hard drive for infections
  - Monitors computer activity
  - Examines new documents that might contain a virus
  - Works by matching to known virus "signatures"
  - Should have signatures updated frequently
- Recommended configuration
  - Constantly monitor for viruses
  - Automatically check for updated signature files
  - See Figure 3-7

# Configuring Personal Firewalls

- Software-based personal firewall
  - Designed to prevent malware from entering a computer
  - Examines incoming data from the Internet or local network
  - Blocks (filters) certain content
- Configuration
  - User can grant or deny permission for specific programs to communicate across network
  - See Figure 3-8

| Function | Personal Firewall | Network Firewall |
|---|---|---|
| Location | Runs on a single computer | Located on edge of the network |
| Scope of protection | Protects only computer on which it is installed | Protects all devices connected to the network |
| Type | Software that runs on computer | Separate hardware device |
| Filtering | Based on programs running on the computer | Provides sophisticated range of filtering mechanisms |

Table 3-4 Personal and network firewalls

# Configuring Personal Firewalls (cont'd.)

- Recommended firewall settings
  - Turn on firewall for all network locations and connections
  - Block all inbound connections
    - Create exceptions for known connections

# User Account Control (UAC)

- User account
  - Indicates privilege level of the user
    - Which files and folders may be accessed
    - What configuration changes may be made
- Three different types of user accounts
  - Guest accounts
    - Allows least computer control
  - Standard accounts
  - Administrator accounts
    - Allows highest level of computer control

# User Account Control (cont'd.)

- User Account Control
  - Alerts user to operating system events
  - Asks explicit permission to perform task
  - Helps prevent Trojan from making unauthorized changes
  - User with administrator account can authorize changes
- Recommended configuration
  - Set UAC level to *Always notify*
  - Give most users standard accounts

| UAC level | Description | Explanation |
|---|---|---|
| Always notify | Users are notified before programs make changes to the computer or to Windows settings that require administrator permissions with secure desktop. | Highest level of security |
| Notify me only when programs try to make changes to my computer | Users are notified through the secure desktop before programs make changes to the computer that requires administrator permissions. Users will not be notified if they try to make changes to Windows settings that require administrator permissions. | Default setting |
| Notify me only when programs try to make changes to my computer (do not dim my desktop) | Users are notified before programs make changes to the computer that requires administrator permissions but not through secure desktop. Users will not be notified if they try to make changes to Windows settings that require administrator permissions. | Other programs might be able to interfere with the visual appearance of the dialog box and could be a security risk, if there are malicious programs running on the computer. |
| Never notify | Users are not notified before any changes are made to the computer. If the user account is administrator level, then programs can make changes to the computer without informing the users. If the user is a standard user any changes that require the permissions of an administrator will automatically be denied. | Least secure setting |

Table 3-5 Microsoft UAC levels and descriptions

# Creating Data Backups

- Copy data from computer's hard drive onto other digital media
  - Store backup in a secure location
- Backups can restore computer to properly functioning state
- Modern operating systems can perform regular, automated backups
- Backup strategy
  - Consider what data should be backed up
  - Consider where the backup should be stored

# Creating Data Backups (cont'd.)

- External portable devices used for backups
  - Portable USB hard drive
  - Disc storage
    - DVD
  - Network-attached storage (NAS)
    - Allows many network devices to access
- Online backup capabilities
  - Automated continuous backup
  - Universal access
  - File feedback information

# Creating Data Backups (cont'd.)

- Online backup capabilities (cont'd.)
  - Optional program file backup
  - Delayed deletion
  - Online or disc-based restore

# Recovering from an Attack

- Preparation
  - Key to recovering from an attack
- Windows systems
  - Create a system repair disc
- Various software vendors provide free rescue discs
  - Downloadable images used to create bootable DVD

# Summary

- Malicious software (malware)
  - Enters a computer system without the owner's knowledge or consent
  - Includes a wide variety of damaging or annoying software
  - Classified according to purpose
    - Spreading, concealing, or profiting
- Viruses and worms are types of spreading malware
- Trojan is a type of concealing malware
- Botnets and spyware are types of profiting malware

# Summary (cont'd.)

- A security patch is a general software security update
- Software-based personal firewall
  - Screens incoming traffic to prevent malware from entering
- Recommended defense: create regular data backups
- Preparation is the key to recovering from an attack