Malware Attacks

Objectives

- Explain types of malware

Introduction

- Malware is software that enters a computer system without the user’s knowledge or consent and then performs an unwanted and usually harmful action.
- Strictly speaking, malware uses a threat vector to deliver a malicious “payload” that performs a harmful function once it is invoked.
- Malware is most often used as a general term that refers to a wide variety of damaging software programs.

Types of mutating malware

- Oligomorphic malware: this malware changes its internal code to one of a set number of predefined mutations whenever it is executed. However, because oligomorphic malware has only a limited number of mutations, it will eventually change back into a previous version that may then be detected by a scanner.

Types of mutating malware

- Polymorphic malware: Malware code that completely changes from its original form whenever it is executed is known as polymorphic malware. This is usually accomplished by the malware containing “scrambled” code that, when the malware is activated, is “unscrambled” before it is executed.

- Metamorphic malware can actually rewrite its own code and thus appears different each time it is executed. It does this by creating a logical equivalent of its code whenever it is run

Understanding Malicious Code (Malware)

- Consists of computer programs designed to break into computers or to create havoc on computers
- Most common types:
  - Circulation/Infection
    - Viruses
    - Worms
    - Trojan horses
  - Concealment
    - Rootkit
  - Collect data
    - Spyware
    - Adware
    - Ransomware
  - Delete data
    - Logic bombs
  - Modify system Security
    - Back doors
  - Launch attacks
    - Zombie and botnet

Viruses

- Programs that secretly attach to another document or program and execute when that document or program is opened
- Might contain instructions that cause problems ranging from displaying an annoying message to erasing files from a hard drive or causing a computer to crash repeatedly

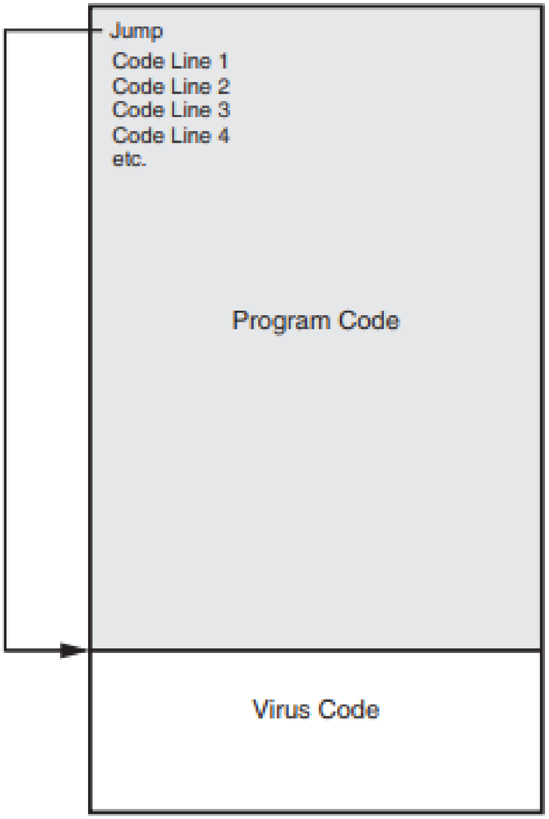


Figure 2-1 Appender infection

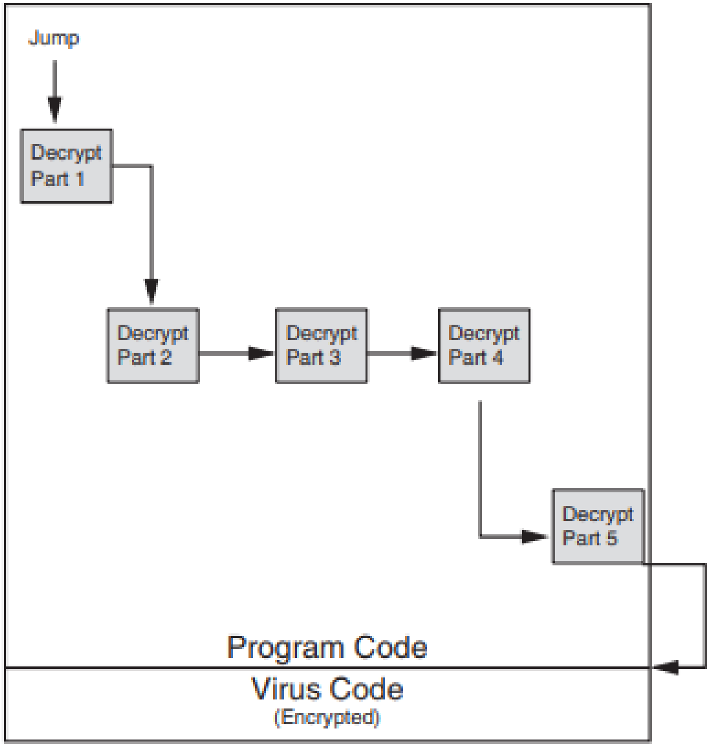


Figure 2-2 Swiss cheese infection

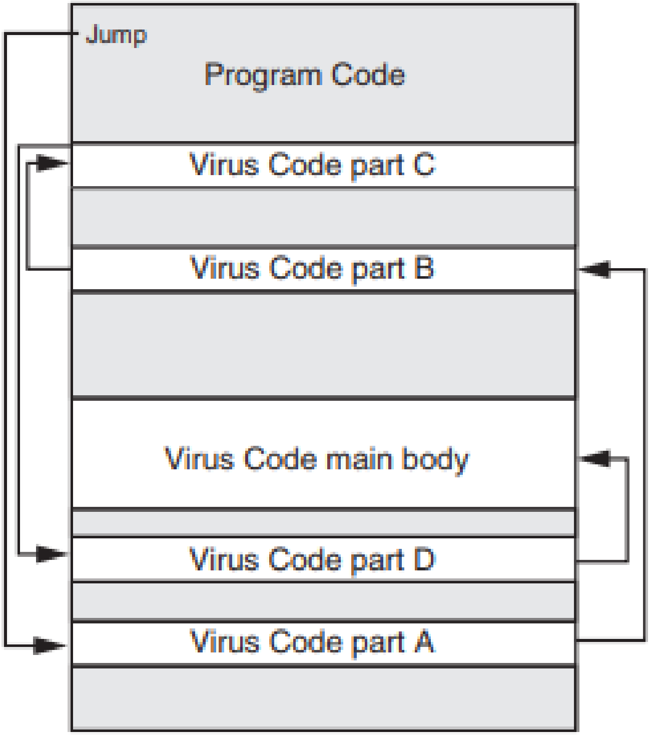


Figure 2-3 Split infection

Viruses (continued)

- Antivirus software defends against viruses is
- Drawback of antivirus software is that it must be updated to recognize new viruses
- Updates (definition files or signature files) can be downloaded automatically from the Internet to a user’s computer

Worms

- Although similar in nature, worms are different from viruses in two regards:
  - A virus attaches itself to a computer document, such as an e-mail message, and is spread by traveling along with the document
  - A virus needs the user to perform some type of action, such as starting a program or reading an e-mail message, to start the infection

Worms (continued)

- Worms are usually distributed via e-mail attachments as separate executable programs
- In many instances, reading the e-mail message starts the worm
- If the worm does not start automatically, attackers can trick the user to start the program and launch the worm

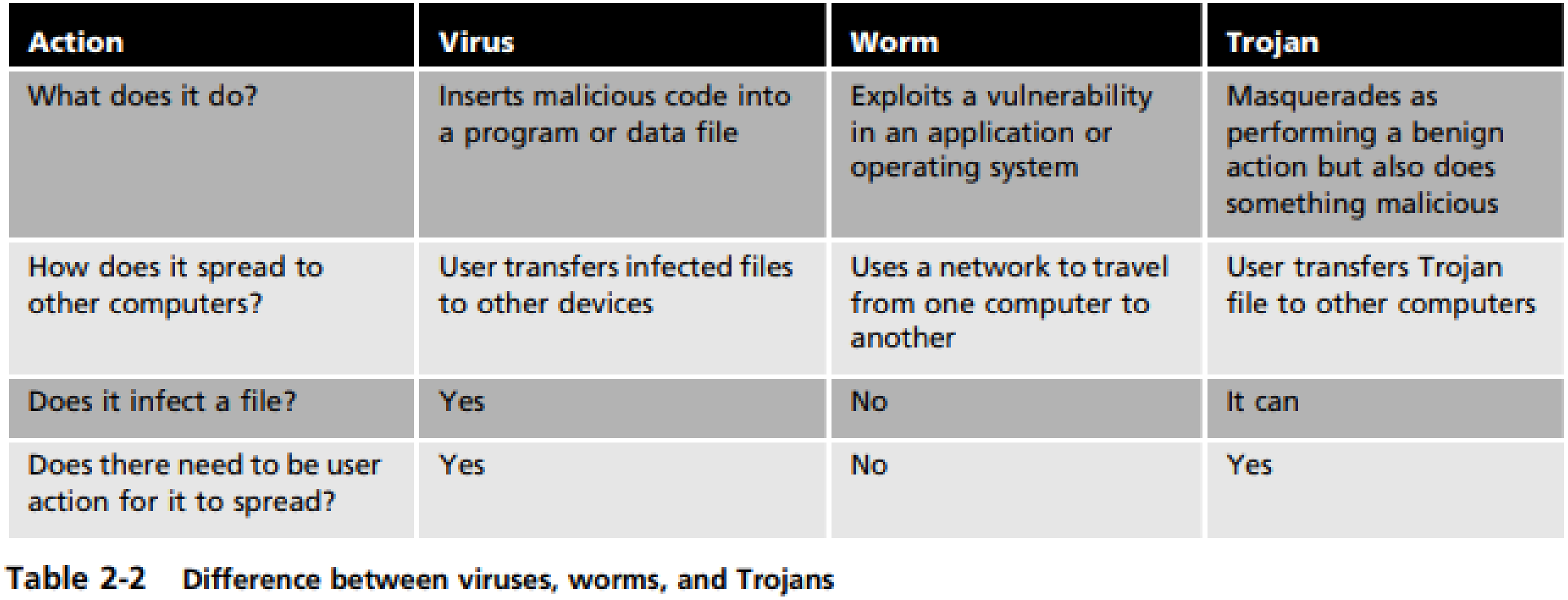
Trojan Horses

- Programs that hide their true intent and then reveals themselves when activated
- Might disguise themselves as free calendar programs or other interesting software
- Common strategies:
  - Giving a malicious program the name of a file associated with a benign program
  - Combining two or more executable programs into a single filename

Trojan Horses (continued)

- Defend against Trojan horses with the following products:
  - Antivirus tools, which are one of the best defenses against combination programs
  - Special software that alerts you to the existence of a Trojan horse program
  - Anti-Trojan horse software that disinfects a computer containing a Trojan horse

Difference between viruses, worms, and Trojans



Action	Virus	Worm	Trojan
What does it do?	Inserts malicious code into a program or data file	Exploits a vulnerability in an application or operating system	Masquerades as performing a benign action but also does something malicious
How does it spread to other computers?	User transfers infected files to other devices	Uses a network to travel from one computer to another	User transfers Trojan file to other computers
Does it infect a file?	Yes	No	It can
Does there need to be user action for it to spread?	Yes	No	Yes

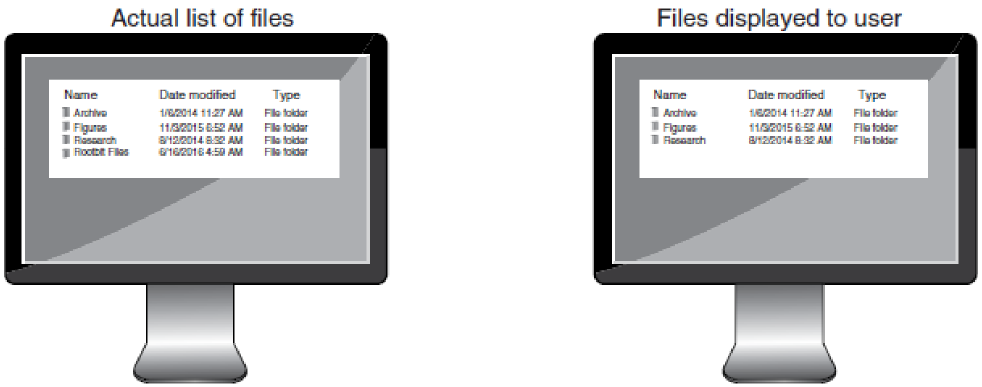
Table 2-2 **Difference between viruses, worms, and Trojans**

Rootkit

- A rootkit is a set of software tools used to hide the actions or presence of other types of software.
- Rootkits do this by changing the operating system to force it to ignore their malicious files or activity.
- Rootkits also hide or remove all traces of evidence that may reveal the malware, such as log entries.

Rootkit

- One approach used by rootkits is to alter or replace operating system files with modified versions that are specifically designed to ignore malicious evidence.
- For example, scanning software may be instructed to scan all files in a specific directory. A rootkit will replace the operating system's accurate list of files with the rootkit's own routine that will not display malicious files



Actual list of files

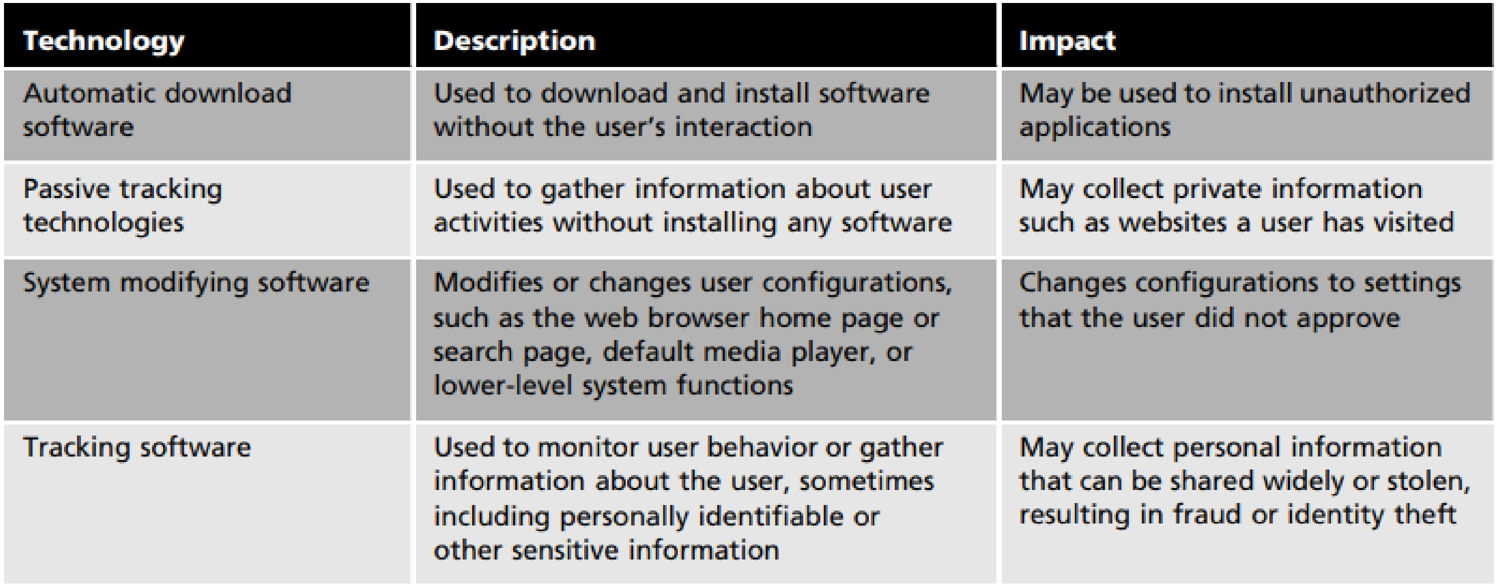
Name	Date modified	Type
Archive	1/6/2014 11:27 AM	File folder
Figures	11/3/2015 6:52 AM	File folder
Research	8/12/2014 8:32 AM	File folder
Rootkit Files	6/16/2016 4:59 AM	File folder

Files displayed to user

Name	Date modified	Type
Archive	1/6/2014 11:27 AM	File folder
Figures	11/3/2015 6:52 AM	File folder
Research	8/12/2014 8:32 AM	File folder

Spyware

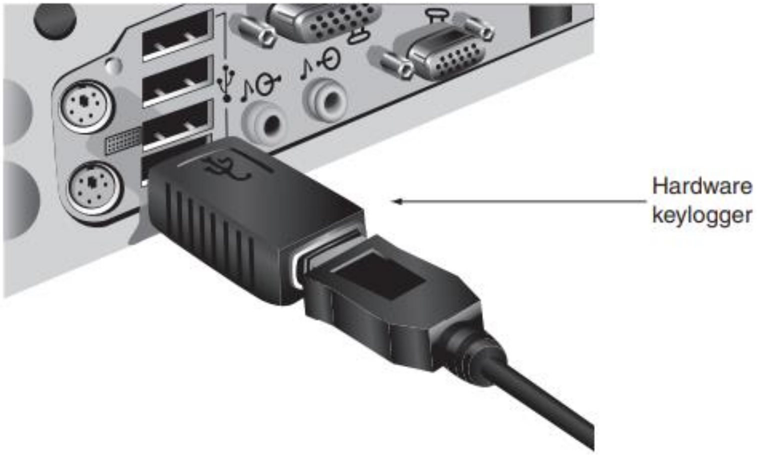
- Spyware is a general term used to describe software that secretly spies on users by collecting information without their consent.



Technology	Description	Impact
Automatic download software	Used to download and install software without the user's interaction	May be used to install unauthorized applications
Passive tracking technologies	Used to gather information about user activities without installing any software	May collect private information such as websites 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	May collect personal information that can be shared widely or stolen, resulting in fraud or identity theft

Spyware - keylogger

- Keylogger that silently captures and stores each keystroke that a user types on the computer's keyboard. The attacker then searches the captured text for any useful information such as passwords, credit card numbers, or personal information.

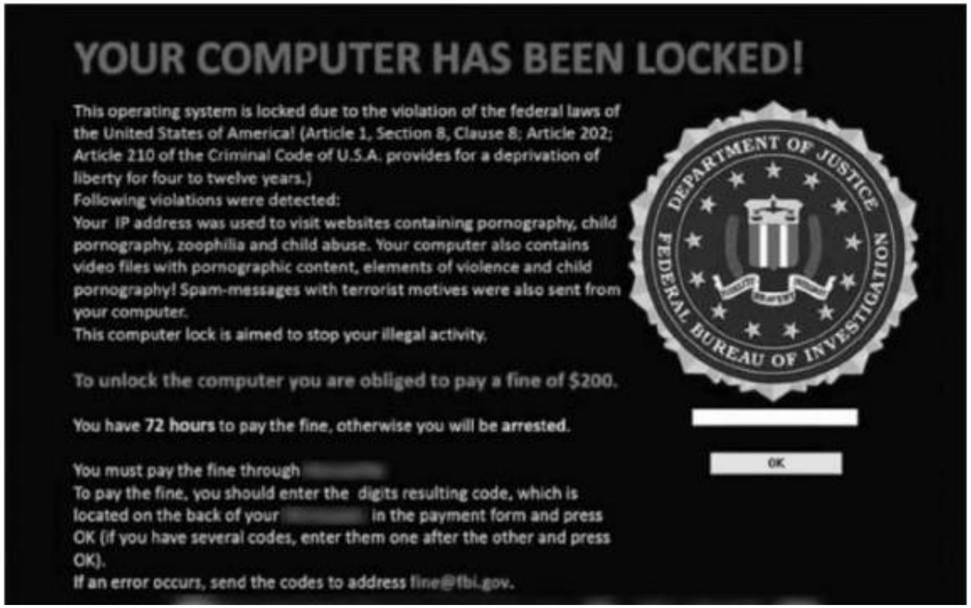


Adware

- Adware delivers advertising content in a manner that is unexpected and unwanted by the user. Once the adware malware becomes installed, it typically displays advertising banners, popup ads, or opens new web browser windows at random intervals

Ransomware

- Ransomware prevents a user’s device from properly operating until a fee is paid.
- One type of ransomware locks up a user’s computer and then displays a message that purports to come from a law enforcement agency



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

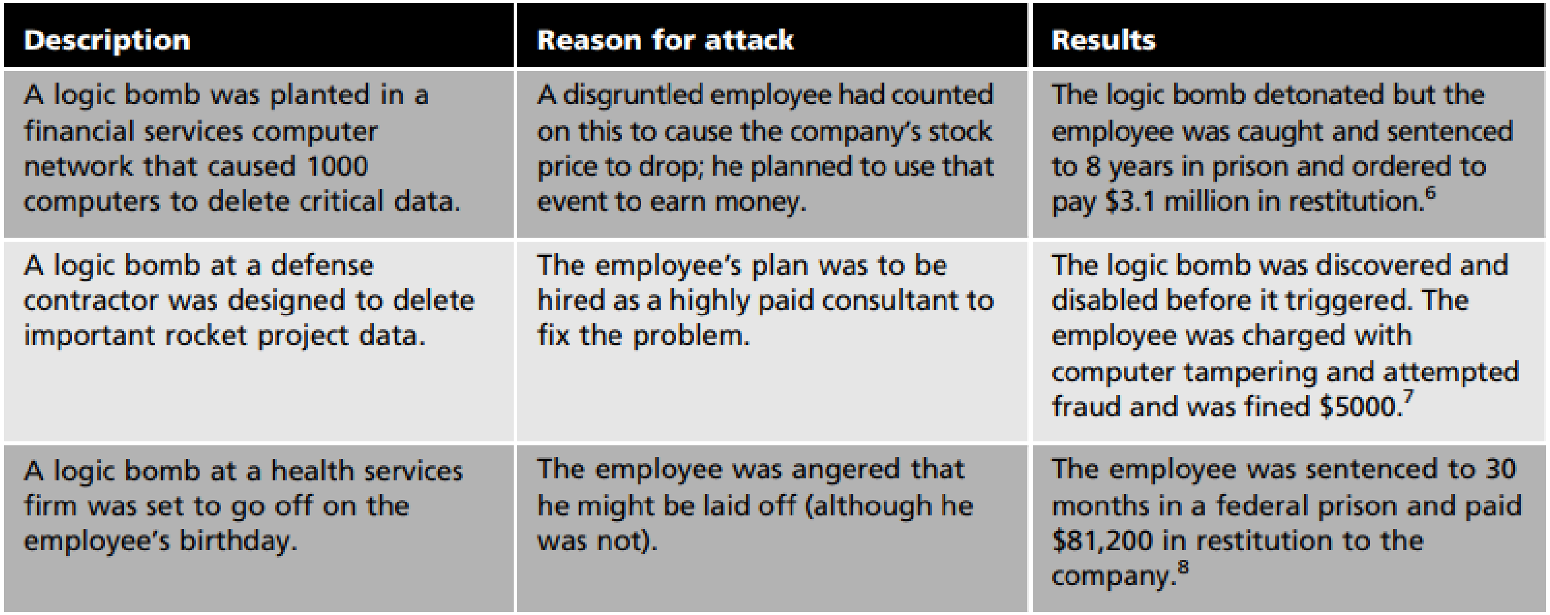
To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Logic Bombs

- Computer program that lies dormant until triggered by a specific event, for example:
  - A certain date being reached on the system calendar
  - A person’s rank in an organization dropping below a specified level



Description	Reason for attack	Results
A logic bomb was planted in a financial services computer network that caused 1000 computers to delete critical data.	A disgruntled employee had counted on this to cause the company’s stock price to drop; he planned to use that event to earn money.	The logic bomb detonated but the employee was caught and sentenced to 8 years in prison and ordered to pay $3.1 million in restitution.[6]
A logic bomb at a defense contractor was designed to delete important rocket project data.	The employee’s plan was to be hired as a highly paid consultant to fix the problem.	The logic bomb was discovered and disabled before it triggered. The employee was charged with computer tampering and attempted fraud and was fined $5000.[7]
A logic bomb at a health services firm was set to go off on the employee’s birthday.	The employee was angered that he might be laid off (although he was not).	The employee was sentenced to 30 months in a federal prison and paid $81,200 in restitution to the company.[8]

Back Doors

- The payload of some types of malware attempts to modify the system’s security settings so that more insidious attacks can be made.
- One type of malware in this category is called a backdoor. A backdoor gives access to a computer, program, or service that circumvents any normal security protections.
- Backdoors that are installed on a computer allow the attacker to return at a later time and bypass security settings.

Zombie and botnet

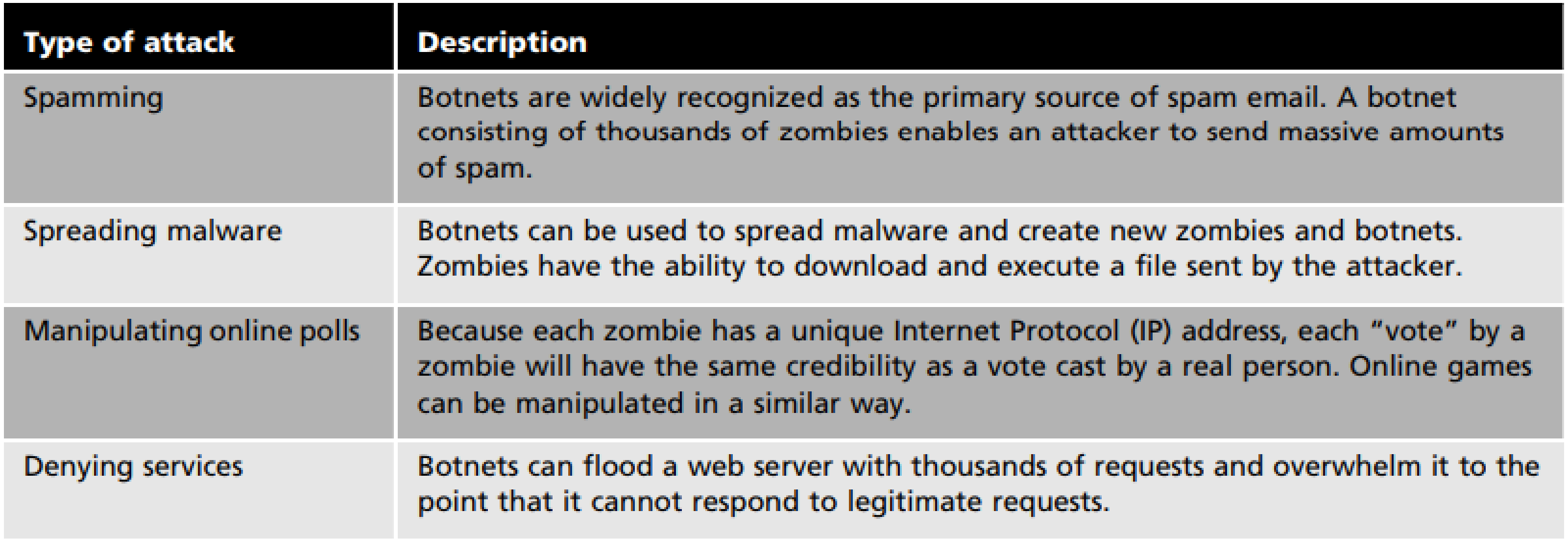
- One of the most popular payloads of malware today carried by Trojans, worms, and viruses is software that will allow the infected computer to be placed under the remote control of an attacker.
- This infected robot (bot) computer is known as a zombie.
- When hundreds, thousands, or even hundreds of thousands of zombie computers are gathered into a logical computer network, they create a botnet under the control of the attacker (bot herder).

Zombie and botnet

- Infected zombie computers wait for instructions through a command and control (C&C or C2) structure from the bot herders regarding which computers to attack and how.
- A common botnet C&C mechanism used today is the Hypertext Transport Protocol (HTTP)

- A zombie can receive its instructions by automatically signing in to a website that the bot herder operates
- Another way to receive instructions is to a third-party website on which information has been placed that the zombie knows how to interpret as commands.
- Some botnets even use blogs or send specially coded attack commands through posts on the Twitter social networking service or notes posted in Facebook.

Uses of botnet



Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam.
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.

Summary

- Six categories of attackers: hackers, crackers, script kiddies, spies, employees, and cyberterrorists
- Identity attacks attempt to assume the identity of a valid user
- Denial of service (DoS) attacks flood a server or device with requests, making it unable to respond to valid requests
- Malicious code (malware) consists of computer programs intentionally created to break into computers or to create havoc on computers