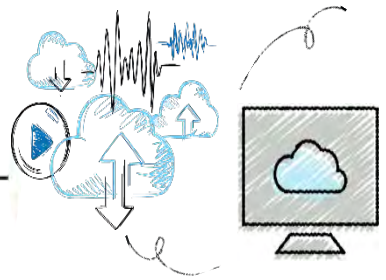
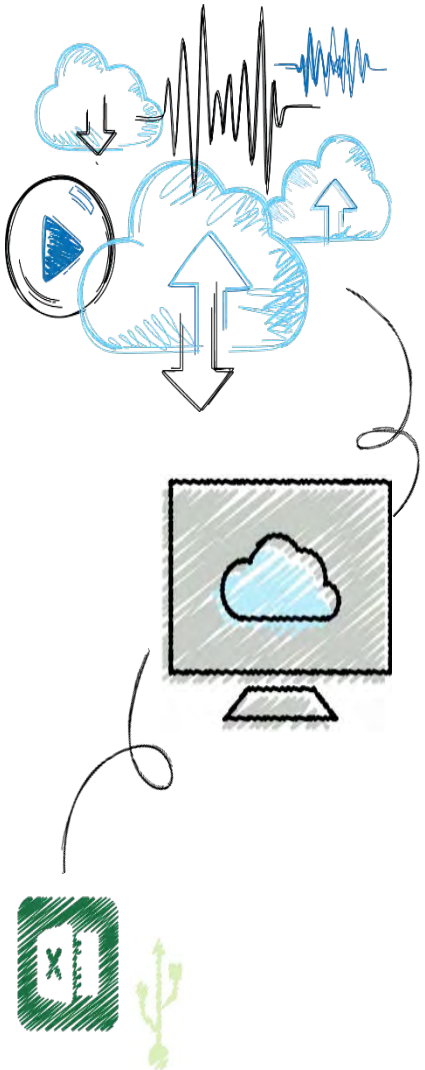
CompTIA Security+

Module 2

Malware and Social Engineering Attacks





Objectives

2.1 Define malware

2.2 List the different types of malware

2.3 Identify payloads of malware

2.4 Describe the types of psychological social engineering attacks

2.5 Explain physical social engineering attacks

Attacks Using Malware (1 of 2)

- Malicious software (malware)
  - Enters a computer system without the owner's knowledge or consent
  - Uses a threat vector to deliver a malicious "payload" that performs a harmful function once it is invoked
- Malware is a general term that refers to a wide variety of damaging or annoying software

Attacks Using Malware (2 of 2)

- Malware can be classified by the using the primary trait that the malware possesses:
  - **Circulation** - spreading rapidly to other systems in order to impact a large number of users
  - **Infection** - how it embeds itself into a system
  - **Concealment** - avoid detection by concealing its presence from scanners
  - **Payload capabilities** - what actions the malware performs

Circulation

- Two types of malware have the primary traits of circulation:
  - Viruses
  - Worms

Virus (1 of 6)

- **Computer virus** - malicious computer code that reproduces itself on the same computer
- **Program virus** - infects an executable program file
- **Macro** - a series of instructions that can be grouped together as a single command
  - Common data file virus is a **macro virus** that is written in a script known as a macro
- Virus infection method:
  - **Appender infection** - virus appends itself to end of a file
    - Easily detected by virus scanners

Virus (2 of 6)

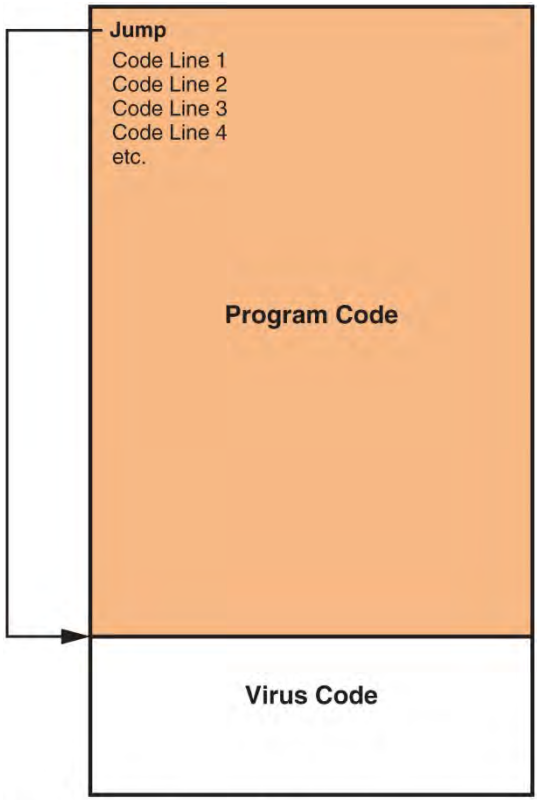


Figure 2-1 Appender infection

Virus (3 of 6)

- Most viruses today go to great lengths to avoid detection (called an armored virus)
- Some armored virus infection techniques include:
  - **Swiss cheese infection** - viruses inject themselves into executable code
    - Virus code is “scrambled” to make it more difficult to detect
  - **Split infection** - virus splits into several parts
    - Parts placed at random positions in host program
    - The parts may contain unnecessary “garbage” doe to mask their true purpose
  - **Mutation** – some viruses can mutate or change
    - An oligomorphic virus changes its internal code to one of a set of number of predefined mutations whenever executed
    - A polymorphic virus completely changes from its original form when executed
    - A metamorphic virus can rewrite its own code and appear different each time it is executed

Virus (4 of 6)

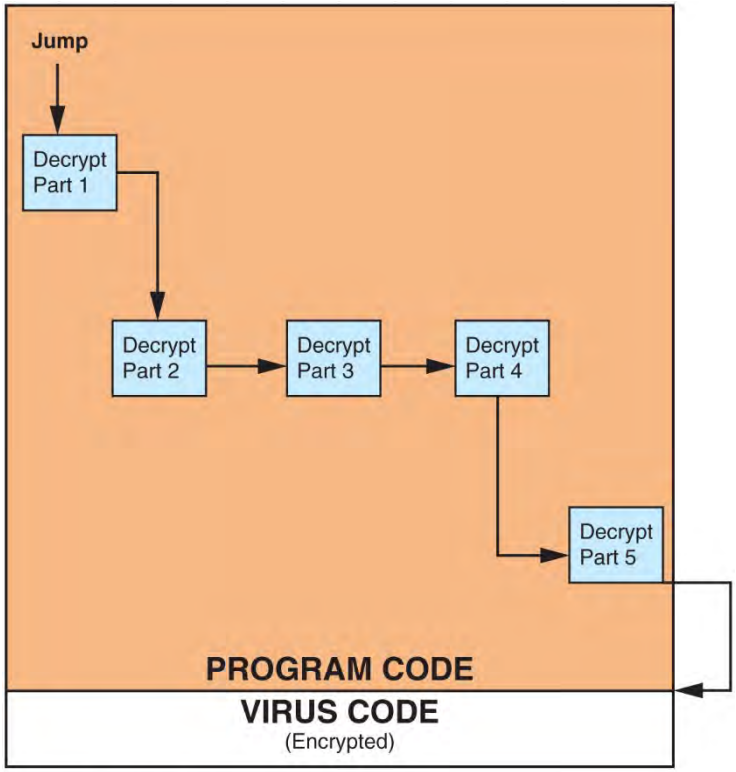


Figure 2-2 Swiss cheese infection

Virus (4 of 6)

- Most viruses today go to great lengths to avoid detection (called an armored virus)
- Some armored virus infection techniques include:
  - **Swiss cheese infection** - viruses inject themselves into executable code
    - Virus code is “scrambled” to make it more difficult to detect
  - **Split infection** - virus splits into several parts
    - Parts placed at random positions in host program
    - The parts may contain unnecessary “garbage” doe to mask their true purpose
  - **Mutation** – some viruses can mutate or change
    - An oligomorphic virus changes its internal code to one of a set of number of predefined mutations whenever executed
    - A polymorphic virus completely changes from its original form when executed
    - A metamorphic virus can rewrite its own code and appear different each time it is executed

Virus (5 of 6)

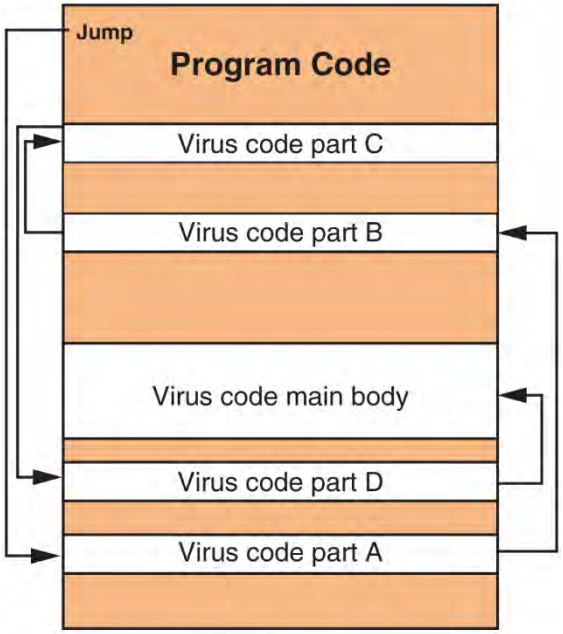


Figure 2-3 Split infection

Virus (5 of 6)

- Most viruses today go to great lengths to avoid detection (called an armored virus)
- Some armored virus infection techniques include:
  - **Swiss cheese infection** - viruses inject themselves into executable code
    - Virus code is “scrambled” to make it more difficult to detect
  - **Split infection** - virus splits into several parts
    - Parts placed at random positions in host program
    - The parts may contain unnecessary “garbage” doe to mask their true purpose
  - **Mutation** – some viruses can mutate or change
    - An oligomorphic virus changes its internal code to one of a set of number of predefined mutations whenever executed
    - A polymorphic virus completely changes from its original form when executed
    - A metamorphic virus can rewrite its own code and appear different each time it is executed

Virus (6 of 6)

- Viruses perform two actions:
  - Unloads a payload to perform a malicious action
  - Reproduces itself by inserting its code into another file on the same computer
- Examples of virus actions
  - Cause a computer to repeatedly crash
  - Erase files from or reformat hard drive
  - Turn off computer's security settings
- Viruses cannot automatically spread to another computer
  - Relies on user action to spread
- Viruses are attached to files
- Viruses are spread by transferring infected files

Worm (1 of 2)

- **Worm** - malicious program that uses a computer network to replicate
  - Sends copies of itself to other network devices
- Worms may:
  - Consume resources **or**
  - Leave behind a payload to harm infected systems
- Examples of worm actions
  - Deleting computer files
  - Allowing remote control of a computer by an attacker

Worm (2 of 2)

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

Infection

- Three examples of malware that have the primary trait of Infection:
  - Trojans
  - Ransomware
  - Crypto-malware

Trojans

- **Trojan -** an executable program that does something other than advertised
  - Contain hidden code that launches an attack
  - Sometimes made to appear as data file
- Examples:
  - User downloads “Free Calendar” or “Free Screensaver”
    - Program scans system for credit card numbers and/or passwords
    - Transmits information to attacker through network

Trojans

- **Trojan -** an executable program that does something other than advertised

- **Special type of Trojan (RAT)**:
  - **R**emote **A**ccess **T**rojan – gives the threat actor unauthorized remote access to the victim's computer by using specially configured communication protocols

Ransomware (1 of 3)

- **Ransomware -** prevents a user's device from properly operating until a fee is paid
  - It is highly profitable
    - Small amount from many users
- Variations of ransomware
  - Claims illegal content has been found (Displays a fake FBI warning)
    - User must pay or go to jail
  - Appears the device is loaded with Viruses and Trojans
    - Users must purchase additional software online to fix the problem

Ransomware (2 of 3)

Figure 2-4 Ransomware message

Source: Symantec Security Response

Ransomware (1 of 3)

- **Ransomware -** prevents a user's device from properly operating until a fee is paid
  - It is highly profitable
    - Small amount from many users
- Variations of ransomware
  - Claims illegal content has been found (Displays a fake FBI warning)
    - User must pay or go to jail
  - Appears the device is loaded with Viruses and Trojans
    - Users must purchase additional software online to fix the problem

Ransomware (3 of 3)

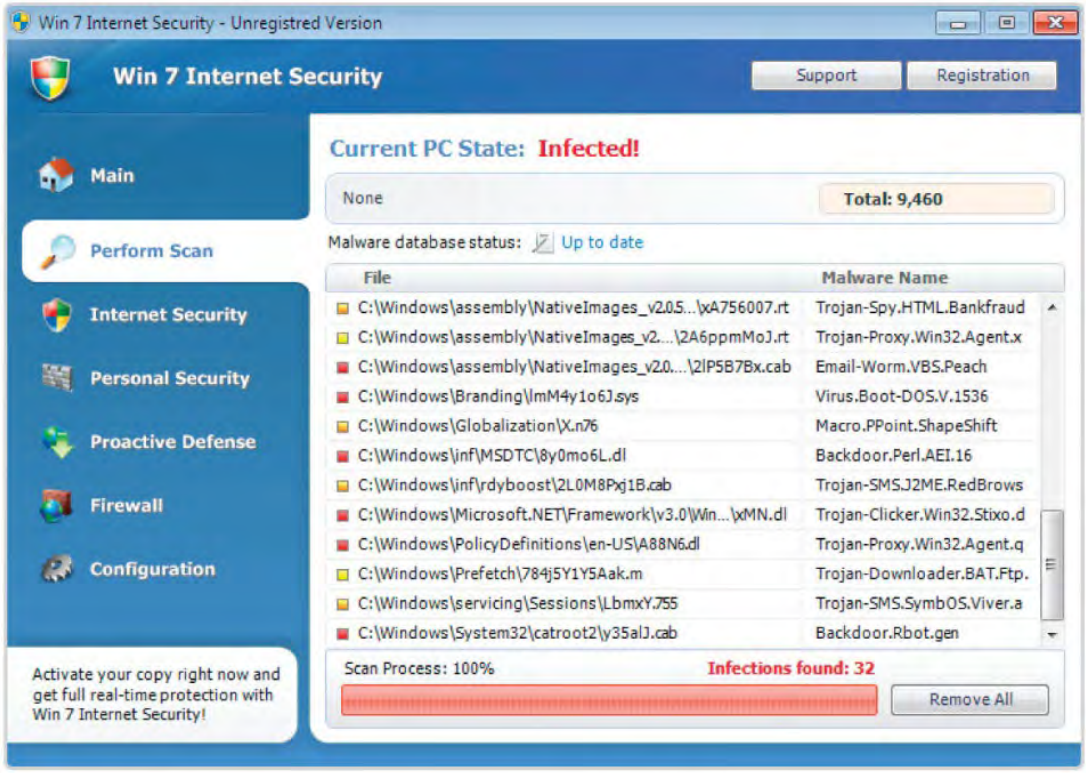


Figure 2-5 Ransomware computer infection

Source: Microsoft Security Intelligence Report

Crypto-malware (1 of 2)

- Crypto-malware – a more malicious form of ransomware where threat actors encrypt all files on the device so that none of them could be opened
- Once infected with crypto-malware:
  - The software connects to the threat actor's command and control (C&C) server to receive instructed or updated data
  - A locking key is generated for the encrypted files and that key is encrypted with another key that has been downloaded from the C&C
  - Second key is sent to the victims once they pay the ransom

Crypto-malware (2 of 2)

Figure 2-6 Crypto-malware message

Source: PC Risk

Concealment (1 of 2)

- **Rootkits** - software tools used by an attacker to hide actions or presence of other types of malicious software
  - Hide or remove traces of log-in records, log entries
- May alter or replace operating system files with modified versions that are specifically designed to ignore malicious activity
- Users can no longer trust their computer that contains a rootkit
  - The rootkit is in charge and hides what is occurring on the computer

Concealment (2 of 2)

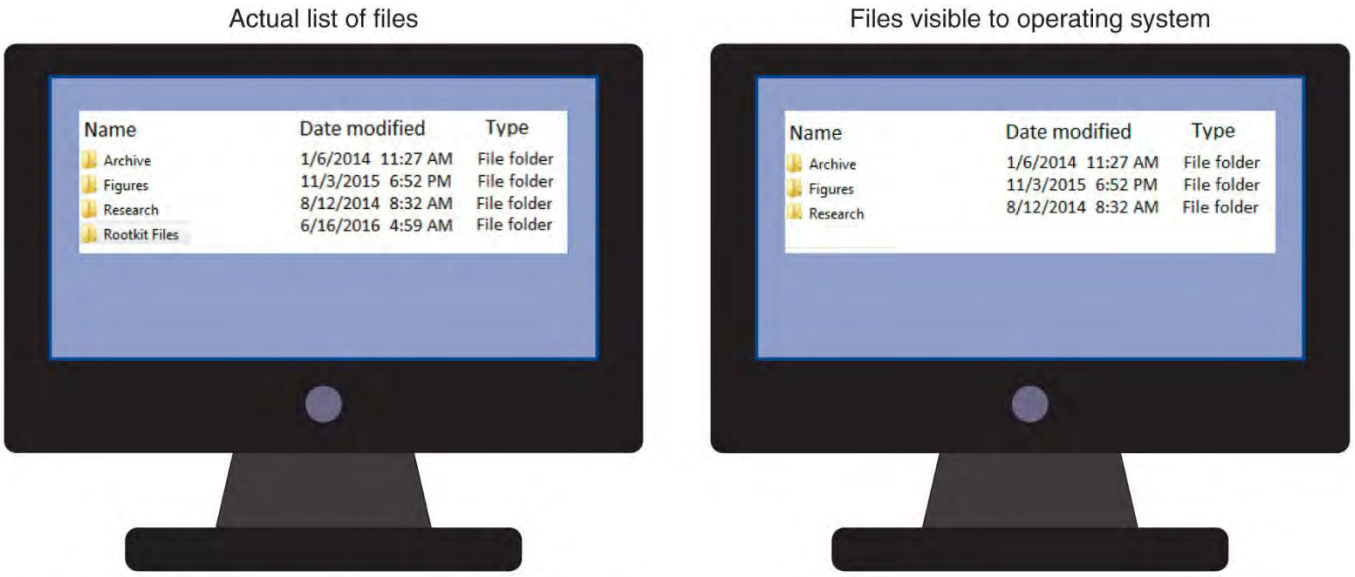


Figure 2-7 Computer infected with rootkit

Payload Capabilities

- The destructive power of malware can be found in its payload capabilities
- Primary payload capabilities are to:
  - Collect data
  - Delete data
  - Modify system security settings
  - Launch attacks

Collect Data (1 of 6)

- Different types of malware are designed to collect important data from the user's computer and make it available at the attacker
- This type of malware includes:
  - Spyware
  - Adware

Collect Data (2 of 6)

- **Spyware** - software that gathers information without user consent
  - Uses the computer's resources for the purposes of collecting and distributing personal or sensitive information
- **Keylogger** - captures and stores each keystroke that a user types on the computer's keyboard
  - Attacker searches the captured text for any useful information such as passwords, credit card numbers, or personal information

Collect Data (3 of 6)

- A keylogger can be a small hardware device or a software program
  - As a Hardware device, it is inserted between the computer keyboard connection and USB port
  - Major Disadvantage:
    - Attacker must physically install it
    - Attacker must physically retrieve it

Collect Data (4 of 6)

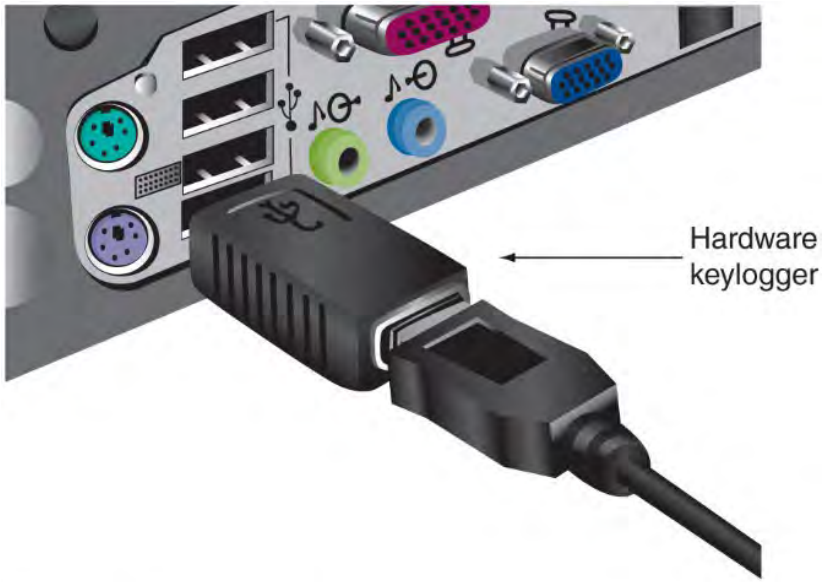


Figure 2-9 Hardware keylogger

Collect Data (5 of 6)

- A keylogger can be a small hardware device or a software program
  - Software keyloggers are programs installed on the computer that silently capture information
- An advantage of software keyloggers is that they do not require physical access to the user's computer
  - Often installed as a Trojan or virus, they can send captured information back to the attacker via Internet

Collect Data (5 of 6)

Figure 2-8 Software keylogger

Source: Ecodsoft

Collect Data (6 of 6)

- **Adware** - program that delivers advertising content in manner unexpected and unwanted by the user
  - Typically displays advertising banners and pop-up ads
  - May open new browser windows randomly
- Users disapprove of adware because:
  - Adware can display objectionable content
  - Frequent popup ads can interfere with a user's productivity
  - Popup ads can slow a computer or even cause crashes and the loss of data
  - Unwanted advertisements can be a nuisance

Delete Data

- The payload of other types of malware deletes data on the computer
- **Logic bomb -** computer code that lies dormant until it is triggered by a specific logical event
  - Difficult to detect before it is triggered
  - Often embedded in large computer programs that are not routinely scanned

Modify System Security

- **Backdoor -** gives access to a computer, program, or service that circumvents normal security to give program access
  - When installed on a computer, they allow the attacker to return at a later time and bypass security settings

Launch Attacks (1 of 2)

- **Bot or zombie** - an infected computer that is under the remote control of an attacker
- Groups of zombie computers are gathered into a logical computer network called a **botnet** under the control of the attacker (**bot herder**)
- Infected zombie computers wait for instructions through a **command and control (C&C)** structure from bot herders
  - A common C&C mechanism used today is HTTP, which is more difficult to detect and block

Launch Attacks (2 of 2)

Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of bots enables an attacker to send massive amounts of spam.
Spreading malware	Botnets can be used to spread malware and create new bots and botnets. Bots can download and execute a file sent by the attacker.
Manipulating online polls	Because each bot has a unique Internet Protocol (IP) address, each “vote” by a bot will have the same credibility as a vote cast by a real person.
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.

Social Engineering Attacks

- **Social engineering -** a means of gathering information for an attack by relying on the weaknesses of individuals
- Social engineering attacks can involve psychological approaches as well as physical procedures

Psychological Approaches

- Psychological approach's goal:
  - To persuade the victim to provide information or take action for the hacker
- Attackers use a variety of techniques to gain trust:
  - Provide a reason (usually an emergency or offer of assistance)
  - Project confidence
  - Use evasion and diversion
  - Make them laugh
- Psychological approaches often involve:
  - Impersonation, phishing, spam, hoaxes, and watering hole attacks

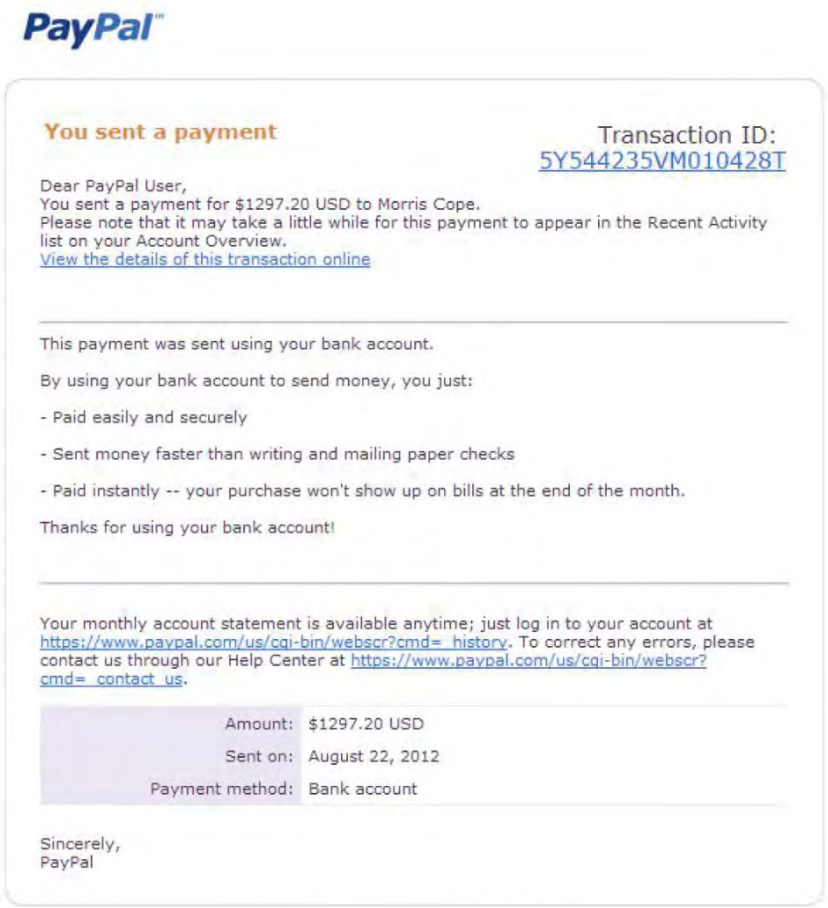
Impersonation

- **Impersonation** - attacker pretends to be someone else:
  - Help desk support technician
  - Repairperson
  - IT support
  - Manager
  - Trusted third party
  - Fellow employee
- Attacker will often impersonate a person with authority because victims generally resist saying “no” to anyone in power

Phishing (1 of 2)

- **Phishing** - sending an email claiming to be from legitimate source
  - Tries to trick user into giving private information
  - The emails and fake websites are difficult to distinguish from those that are legitimate
- Variations on phishing attacks:
  - Spear phishing – targets specific users
  - Whaling – targets the “big fish”
  - Vishing – instead of using email, uses a telephone call instead
- About 97% of all attacks start with phishing

Phishing (2 of 2)



PayPal

You sent a payment

Transaction ID:
5Y544235VM010428T

Dear PayPal User,
You sent a payment for $1297.20 USD to Morris Cope.
Please note that it may take a little while for this payment to appear in the Recent Activity list on your Account Overview.
View the details of this transaction online

This payment was sent using your bank account.

By using your bank account to send money, you just:

- Paid easily and securely

- Sent money faster than writing and mailing paper checks

- Paid instantly -- your purchase won't show up on bills at the end of the month.

Thanks for using your bank account!

Your monthly account statement is available anytime; just log in to your account at https://www.paypal.com/us/cgi-bin/webscr?cmd=_history. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/cgi-bin/webscr?cmd=_contact_us.

Amount:	$1297.20 USD
Sent on:	August 22, 2012
Payment method:	Bank account

Sincerely,
PayPal

Figure 2-10 Phishing email message

Source: Email sent to Dr. Mark Revels

Spam (1 of 2)

- **Spam** - unsolicited e-mail
  - Primary vehicles for distribution of malware
  - Sending spam is a lucrative business
    - Cost spammers very little to send millions of spam messages
- Filters look for specific words and block the email
- **Image spam** - uses graphical images of text in order to circumvent text-based filters
  - Often contains nonsense text so it appears legitimate

Spam (2 of 2)

Figure 2-11 Image spam

Hoaxes

- **Hoaxes -** a false warning, usually claiming to come from the IT department
- Attackers try to get victims to change configuration settings on their computers that would allow the attacker to compromise the system
- Attackers may also provide a telephone number for the victim to call for help, which will put them in direct contact with the attacker

Watering Hole Attack

- **Watering hole attack** - a malicious attack that is directed toward a small group of specific individuals who visit the same website
- Example:
  - Major executives working for a manufacturing company may visit a common website, such as a parts supplier to the manufacturer

Physical Procedures

- Two of the most common physical procedures are:
  - Dumpster diving
  - Tailgating

Dumpster Diving (1 of 2)

- **Dumpster diving**
  - Digging through trash to find information that can be useful in an attack
- An electronic variation of dumpster diving is to use Google's search engine to look for documents and data posted online
  - Called **Google dorking**

Dumpster Diving (2 of 2)

Item retrieved	Why useful
Calendars	A calendar can reveal which employees are out of town at a particular time
Inexpensive computer hardware, such as USB flash drives or portal hard drives	Often improperly disposed of and might contain valuable information
Memos	Seemingly unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation
Organizational charts	These identify individuals within the organization who are in positions of authority
Phone directories	Can provide the names and telephone numbers of individuals in the organization to target or impersonate
Policy manuals	These may reveal the true level of security within the organization
System manuals	Can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities

Tailgating

- **Tailgating**
  - Following behind an authorized individual through an access door
  - An employee could conspire with an unauthorized person to allow him to walk in with him (called piggybacking)
  - Watching an authorized user enter a security code on a keypad is known as **shoulder surfing**

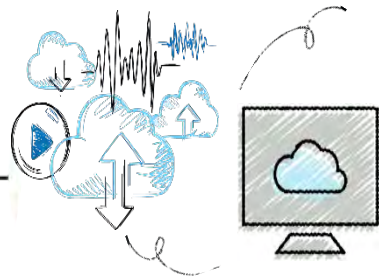
Chapter Summary (1 of 2)

- Malware is malicious software that enters a computer system without the owner's knowledge or consent
- Malware that spreads include computer viruses and worms
- Ransomware prevents a user's device from properly and fully functioning until a fee is paid
- A rootkit can hide its presence or the presence of other malware on the computer by accessing lower layers of the OS
- Different types of malware are designed to collect data from the user's computer and make it available to the attacker
  - Spyware, keylogger, and adware

Chapter Summary (2 of 2)

- A logic bomb is computer code that is typically added to a legitimate program but lies dormant until triggered by a specific logical event
- A backdoor gives access to a computer, program, or service that circumvents any normal security protections
- A popular payload of malware is software that will allow the infected computer to be placed under the remote control of an attacker (known as a bot)
  - Multiple bot computers can be used to created a botnet
- Social engineering is a means of gathering information for an attack from individuals
- Types of social engineering approaches include phishing, dumpster diving, and tailgating

SOCIAL ENGINEERING TEST



Phishing Sites: Which is Which???

- http://www.bankofamerica.com/accounts
- http://www.bankofamerica.co/accounts
- https://www.bankoamerica.com/accounts
- https://www.bankofamerica.com/accounts
- http://www.arvest.con/passwordreset
- https://www.arvest.com/passwordreset
- https://www.arvest.com/passswordreset
- https://www.arwest.com/passwordreset

Phishing Sites: Which is Which???

- https://www.bankofamerica.com/accounts
- http://www.bankofamerica.com/accounts
- https://www.bankofamerica.com/accounts
- https://www.bankofamerica.com/accounts
- http://www.arvest.con/passwordreset
- https://www.arvest.com/passwordreset
- https://www.arvest.com/passswordreset
- https://www.arwest.com/passwordreset

Review Questions

Which of the following is not a primary trait of malware?

A. diffusion

B. circulation

C. infection

D. concealment

Review Questions

Which of the following is not a primary trait of malware?

A. **diffusion**

B. circulation

C. infection

D. concealment

Review Questions

Which type of malware requires a user to transport it from one computer to another?

A. worm

B. rootkit

C. adware

D. virus

Review Questions

Which type of malware requires a user to transport it from one computer to another?

A. worm

B. rootkit

C. adware

D. **virus**

Review Questions

Which type of mutation completely changes a virus from its original form by rewriting its own code whenever it is executed?

A. betamorphic

B. oligomorphic

C. polymorphic

D. metamorphic

Review Questions

Which type of mutation completely changes a virus from its original form by rewriting its own code whenever it is executed?

A. betamorphic

B. oligomorphic

C. polymorphic

D. **metamorphic**

Review Questions

Ebba received a message from one of her tech support employees. In violation of company policy, a user had downloaded a free program to receive weather reports, but the program had also installed malware on the computer that gave the threat actor unrestricted access to the computer. What type of malware had been downloaded?

A. virus

B. ransomware

C. RAT

D. Trojan

Review Questions

Ebba received a message from one of her tech support employees. In violation of company policy, a user had downloaded a free program to receive weather reports, but the program had also installed malware on the computer that gave the threat actor unrestricted access to the computer. What type of malware had been downloaded?

A. virus

B. ransomware

C. **RAT**

D. Trojan

Review Questions

Astrid's computer screen suddenly says that all files are now locked until money is transferred to a specific account, at which time she will receive a means to unlock the files. What type of malware has infected her computer?

A. Bitcoin malware

B. Crypto-malware

C. Blocking virus

D. Networked worm

Review Questions

Astrid's computer screen suddenly says that all files are now locked until money is transferred to a specific account, at which time she will receive a means to unlock the files. What type of malware has infected her computer?

A. Bitcoin malware

B. **Crypto-malware**

C. Blocking virus

D. Networked worm

Review Questions

Helen pretends to be the help desk manager and calls Steve to trick him into giving her his password. What social engineering attack has Helen performed?

A. aliasing

B. duplicity

C. impersonation

D. luring

Review Questions

Helen pretends to be the help desk manager and calls Steve to trick him into giving her his password. What social engineering attack has Helen performed?

A. aliasing

B. duplicity

C. **impersonation**

D. luring

Review Questions

What is the term used for a threat actor who controls multiple bots in a botnet?

A. bot herder

B. zombie shepherd

C. rogue IRC

D. cyber-robot

Review Questions

What is the term used for a threat actor who controls multiple bots in a botnet?

A. **bot herder**

B. zombie shepherd

C. rogue IRC

D. cyber-robot

Coming Up Next…

CompTIA Security+

Module 3

Basic Cryptography