Information Security (CP3404)

Chapter 2 – Malware and Social Engineering Attacks

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

JAMES COOK UNIVERSITY
AUSTRALIA

Learning Objectives

- Define malware
- List the types of malware
- Identify payloads of malware
- Describe the types of social engineering psychological attacks
- Explain physical social engineering attacks

Outline

1. Attacks Using Malware

2. Social Engineering Attacks

Preface

Successful attacks on computers today generally consists of two elements:

1. Malicious software programs (Malwares) that are created by attackers to silently infiltrate computers with the intent to do harm.
2. Tricking users into performing a compromising action or providing sensitive information (a.k.a. Social Engineering).

This chapter examines attacks using these two elements.

Attacks Using Malware

Malware

- Malware (malicious software) – Software that enters a computer system without the owners knowledge or consent
- Refers to a wide variety of damaging or annoying software (e.g., intercept data, steal information, launch other attacks)
- In order to detect malware on an infected computer, a software scanning tool can search for the malware, looking to match it against a known pattern of malware

Attacks Using Malware

Mutating Malware

- Attackers can mask the presence of their malware by having it *mutate* or change
- Three (3) types of mutating malware are:
  1. Oligomorphic malware – Changes its internal code to one of a set number of predefined mutations whenever executed
  2. Polymorphic malware – Completely changes from its original form whenever it is executed
  3. Metamorphic malware – Can actually rewrite its own code and thus appears different each time it is executed

Attacks Using Malware

- Definitions of the different types of malware are often confusing and may overlap

- One method of classifying various types of malware is using four (4) primary traits that malware possesses:

  1. Circulation
  2. Infection
  3. Concealment
  4. Payload capabilities

Attacks Using Malware

Malware Traits

1. Circulation – Some malware has primary trait of spreading rapidly to other systems to impact large number users
2. Infection – Some malware has primary trait of *infect* or embed itself into that system
3. Concealment – Some malware has as its primary trait avoiding detection by concealing its presence from scanners
4. Payload capabilities – When payload capabilities are the primary focus of malware, the focus is on what nefarious action(s) the malware performs

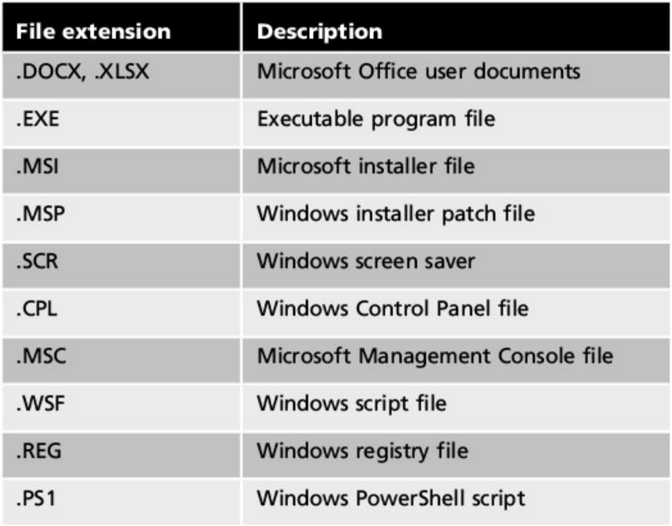
Attacks Using Malware

Three (3) types of malware have the primary traits of circulation and/or infection.

1. Computer virus – Malicious computer code that reproduces itself on the same computer
2. Program virus – Virus that infects an executable program file
3. Macro virus – One of most common data file viruses written in a script known as a macro (macro is series of instructions that can be grouped together as single command).

Table 2-1 lists some of the 70 different Microsoft Windows file types can be infected with a virus

Attacks Using Malware



File extension	Description
.DOCX, .XLSX	Microsoft Office user documents
.EXE	Executable program file
.MSI	Microsoft installer file
.MSP	Windows installer patch file
.SCR	Windows screen saver
.CPL	Windows Control Panel file
.MSC	Microsoft Management Console file
.WSF	Windows script file
.REG	Windows registry file
.PS1	Windows PowerShell script

Table 2-1 Windows file types that can be infected

Attacks Using Malware

One basic type of infection is the appender infection:

- Virus appends itself to end of a file
- Replaces beginning of file with jump instruction pointing to the virus code (see Figure 2-1)
- These types of viruses could easily be detected by virous scanner

Attacks Using Malware

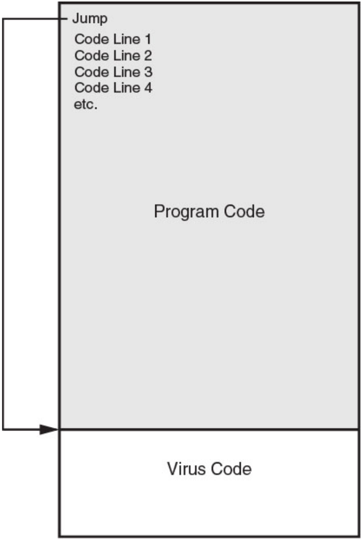


Figure 2-1 Appender infection

Attacks Using Malware

Armored Viruses

Most viruses today go to great lengths to avoid detection. this type of virus is called an armored virus (e.g., Swiss cheese infection and split infection viruses)

- Swiss cheese infection – Encrypts virus code and then divide decryption engine into different pieces and inject these pieces throughout the infected program code (see Figure 2-2)

Attacks Using Malware

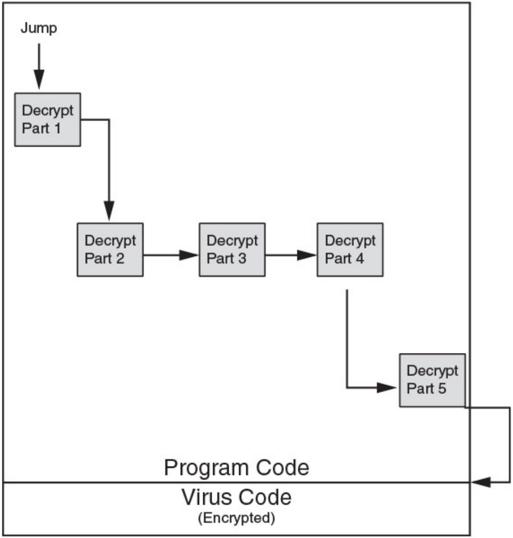


Figure 2-2 Swiss cheese infection

Attacks Using Malware

Armored Viruses (Cont.)

- Split infection – Viruses split the malicious code itself into several parts:
  - Also has one main body of code
  - All parts are placed at random positions throughout the program code
- To make detection even more difficult these parts may contain unnecessary *garbage* code to mask their true purpose (see Figure 2-3)

Attacks Using Malware

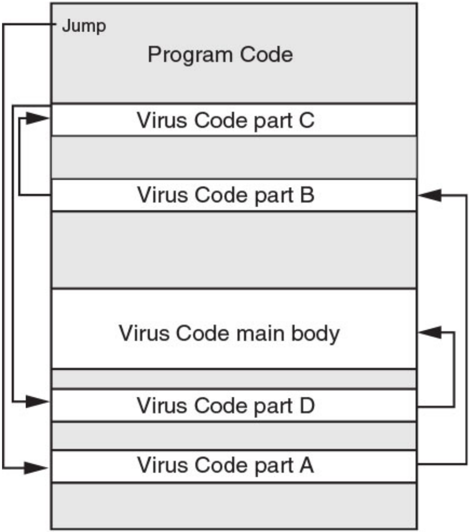


Figure 2-3 Split infection

Attacks Using Malware

Virus Acctions

- When infected program is launched it activates its malicious payload
- Viruses may display an annoying message but usually much more harmful, e.g.:
  - Cause a computer to crash repeatedly
  - Erase files from or reformat hard drive
  - Turn off computers security settings
- Virus also replicates itself by spreading to another file on same computer

Attacks Using Malware

Virus Carriers

- Virus cannot automatically spread to another computer
- Relies on user action to spread
- Viruses are attached to files
- Viruses are spread by transferring infected files
- Virus must have two (2) *carriers*:
  1. File to which it attaches
  2. Human to transport it to other computers

Attacks Using Malware

Worm

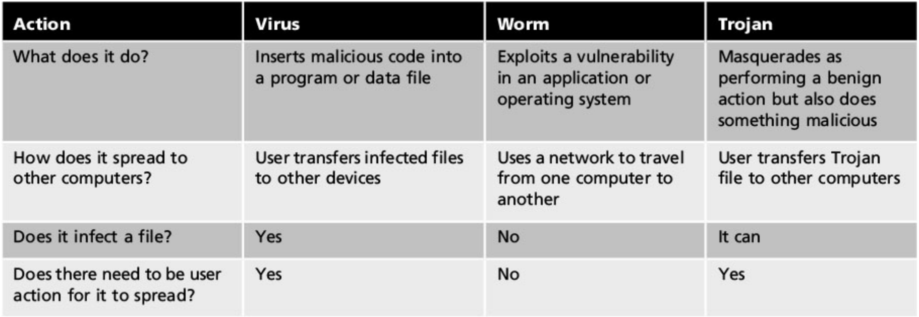
- Malicious program that uses a computer network to replicate
- Sometimes called network viruses
- Worm designed to enter computer through network and then take advantage of vulnerability in application or operating system on host computer
- Once worm exploits vulnerability on one system it immediately searches for another computer on the network that has same vulnerability

Attacks Using Malware

Trojan

- Program that does something other than advertised
- Example:
  - User downloads *free calendar program*
  - Program scans system for credit card numbers and passwords
  - Transmits information to attacker through network

Attacks Using Malware



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

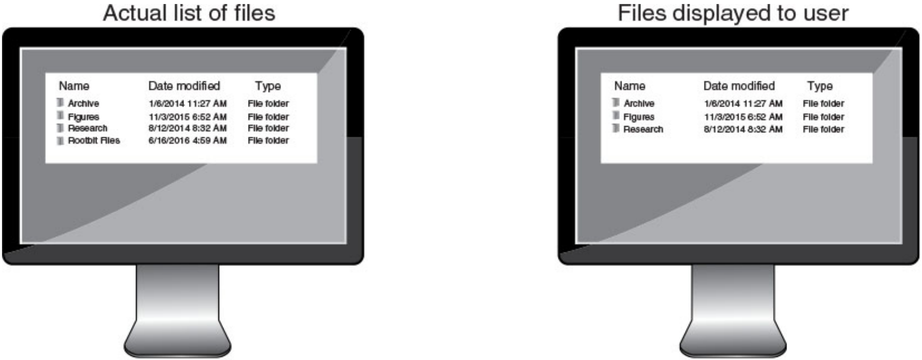
Table 2-2 Difference between viruses, worms, and Trojans

Attacks Using Malware

Rootkit (Concealment)

- Software tools used by an attacker to hide actions or presence of other types of malicious software
- Will hide or remove traces of log-in records, log entries
- May alter or replace operating system files with modified versions specifically designed to ignore malicious activity
- Can be difficult to detect a rootkit or clean it from an infected system

Attacks Using Malware



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

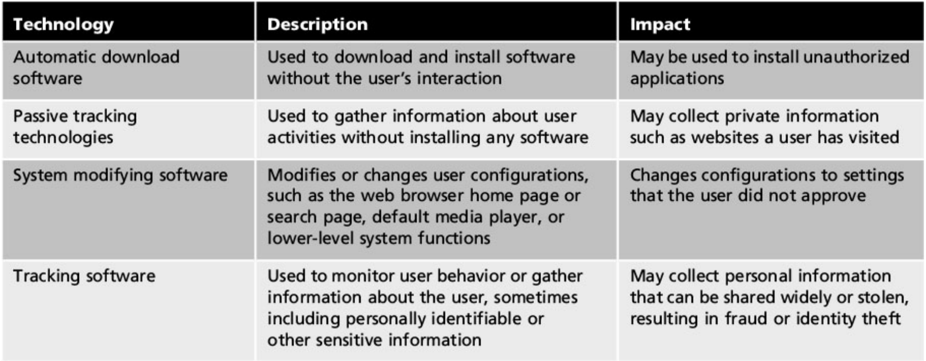
Figure 2-4 Computer infected with rootkit

Attacks Using Malware

Spyware (Payload Capabilities – Collect Data)

- Software that gathers information without user consent
- Spyware is tracking software that is deployed without:
    - Adequate notice
    - Consent
    - Control by the user

Attacks Using Malware



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

Table 2-3 Technologies used by spyware

Attacks Using Malware

Keylogger (Payload Capabilities – Collect Data)

- One type of spyware is a keylogger that captures users keystrokes
- Information later retrieved by attacker
- Attacker searches for useful information
- Can be either small hardware device or software program
- Keyloggers can go beyond capture keystrokes; can also make screen captures and turn on computers web camera to record images of user

Attacks Using Malware

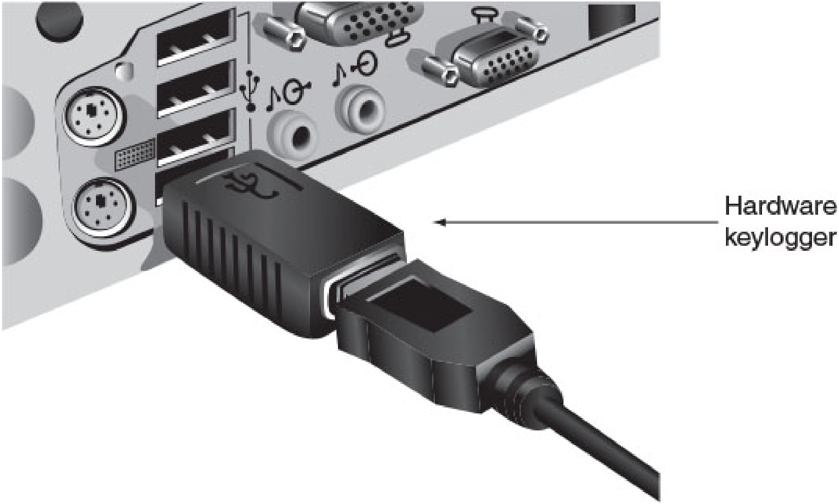


Figure 2-5 Hardware keylogger

Attacks Using Malware

Adware (Payload Capabilities – Collect Data)

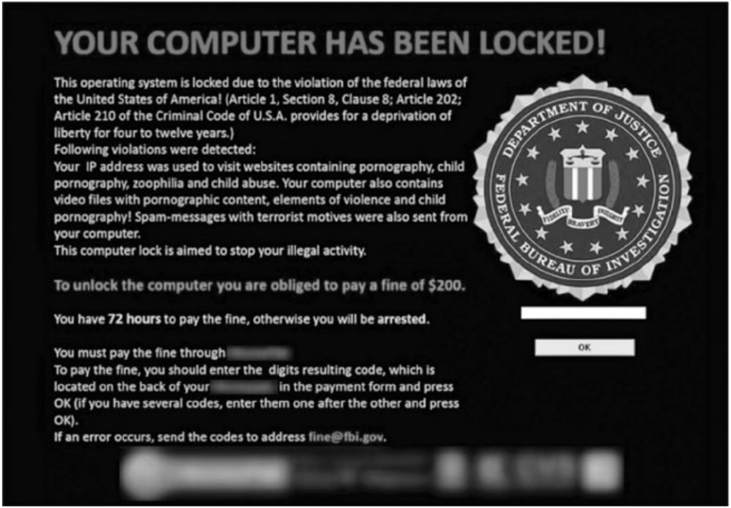
- Program that delivers advertising content in manner unexpected and unwanted by the user
- Downsides of adware for users:
  - May display objectionable content
  - Frequent pop-up ads cause lost productivity
  - Pop-up ads slow computer or cause crashes
  - Unwanted ads can be a nuisance
- Can also perform tracking of online activities

Attacks Using Malware

Ransomware (Payload Capabilities – Collect Data)

- Program that prevents a user's device from properly operating until a fee is paid
- Ransomware malware is highly profitable
- Variation of ransomware displays a fictitious warning that there is a problem with the computer
- No matter what the condition of the computer, the ransomware always reports that there is a problem

Attacks Using Malware



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.

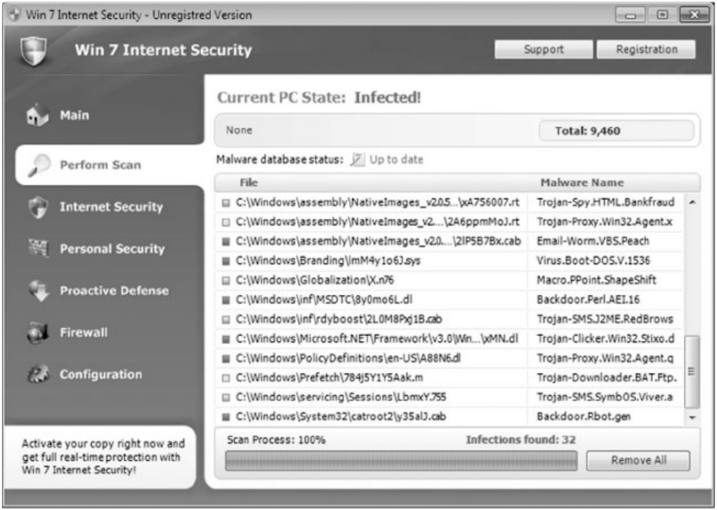
You have **72 hours** to pay the fine, otherwise you will be **arrested**.

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.

Figure 2-6 Ransomware message

Source: Symantec Security Response

Attacks Using Malware



Current PC State: Infected!

None Total: 9,460

Malware database status: Up to date

File	Malware Name
C:\Windows\assembly\NativeImages_v2.0.5...\xA756007.rt	Trojan-Spy.HTML.Bankfraud
C:\Windows\assembly\NativeImages_v2....\2A6ppmMoJ.rt	Trojan-Proxy.Win32.Agent.x
C:\Windows\assembly\NativeImages_v2.0....\2lP5B7Bx.cab	Email-Worm.VBS.Peach
C:\Windows\Branding\lmM4y1o6J.sys	Virus.Boot-DOS.V.1536
C:\Windows\Globalization\X.n76	Macro.PPoint.ShapeShift
C:\Windows\inf\MSDTC\8y0mo6L.dl	Backdoor.Perl.AEI.16
C:\Windows\inf\rdyboost\2L0M8Pxj1B.cab	Trojan-SMS.J2ME.RedBrows
C:\Windows\Microsoft.NET\Framework\v3.0\Win...\xMN.dl	Trojan-Clicker.Win32.Stixo.d
C:\Windows\PolicyDefinitions\en-US\A88N6.dl	Trojan-Proxy.Win32.Agent.q
C:\Windows\Prefetch\784j5Y1Y5Aak.m	Trojan-Downloader.BAT.Ftp.
C:\Windows\servicing\Sessions\LbmxY.755	Trojan-SMS.SymbOS.Viver.a
C:\Windows\System32\catroot2\y35alJ.cab	Backdoor.Rbot.gen

Scan Process: 100% Infections found: 32

Activate your copy right now and get full real-time protection with Win 7 Internet Security!

Figure 2-7 Ransomware computer infection

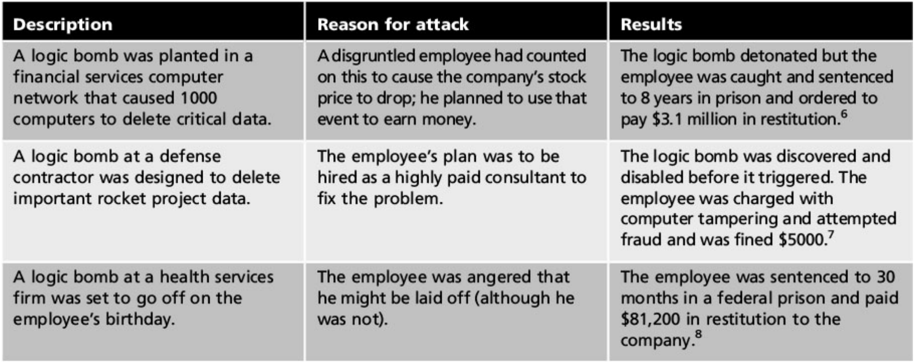
Source: Microsoft Security Intelligence Report

Attacks Using Malware

Logic Bomb (Payload Capabilities – Delete Data)

- Computer code that lies dormant until triggered by a specific logical event and then performs malicious activities
- Difficult to detect before it is triggered
- Logic bombs are often embedded in very large computer programs
- Trusted employee can easily insert a few lines of computer code into a long program without anyone detecting it

Attacks Using Malware



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]

Table 2-4 **Famous logic bombs**

Attacks Using Malware

Backdoor (Payload Capabilities – Modify System Security)

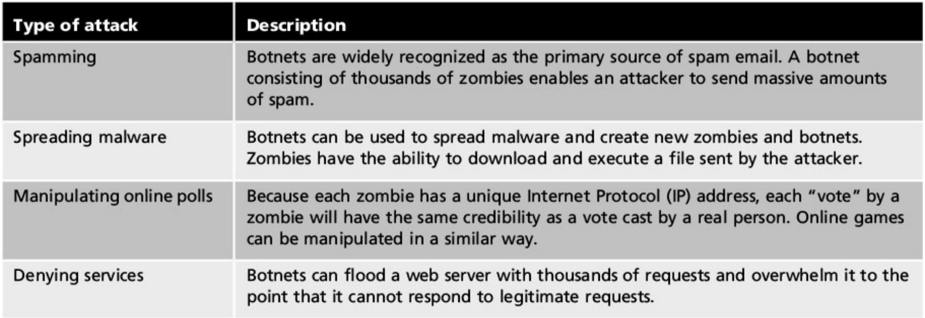
- Software code that circumvents normal security to give program access
- Common practice by developers
- Intent is to remove backdoors in final application but often overlooked

Attacks Using Malware

Zombies and Botnets (Payload Capabilities – Launch Attacks)

- Zombie – Infected robot (bot) computer
- Botnet – Multiple zombie computers gathered into a logical computer network
- Bot herder – Attacker who controls bonet
- Command and control (C&C or C2) – Instructions from the bot herders regarding which computers to attack and how
- Common C&C mechanism used today is Hypertext Transport Protocol (HTTP)

Attacks Using Malware



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.

Table 2-5 Uses of botnets

Quick Quiz

1. A(n) _______ is a series of instructions that can be grouped together as a single command.
   Answer:

Quick Quiz

1. A(n) ______ is a series of instructions that can be grouped together as a single command.
   Answer: macro

Quick Quiz

1. A(n) ______ is a series of instructions that can be grouped together as a single command.
   Answer: macro

2. A(n) ______ is a malicious program designed to enter a computer through the network and then take advantage of vulnerability in an application or an operating system on the host computer.
   Answer:

Quick Quiz

1. A(n) ______ is a series of instructions that can be grouped together as a single command.
   Answer: macro

2. A(n) ______ is a malicious program designed to enter a computer through the network and then take advantage of vulnerability in an application or an operating system on the host computer.
   Answer: worm

Quick Quiz

1. A(n) ______ is a series of instructions that can be grouped together as a single command.
   Answer: macro

2. A(n) ______ is a malicious program designed to enter a computer through the network and then take advantage of vulnerability in an application or an operating system on the host computer.
   Answer: worm

3. A(n) ______ is a set of software tools used by an intruder to break into a computer, obtain special privileges to perform unauthorized functions, and then hide all traces of its existence.
   Answer:

Quick Quiz

1. A(n) ______ is a series of instructions that can be grouped together as a single command.
   Answer: macro

2. A(n) ______ is a malicious program designed to enter a computer through the network and then take advantage of vulnerability in an application or an operating system on the host computer.
   Answer: worm

3. A(n) ______ is a set of software tools used by an intruder to break into a computer, obtain special privileges to perform unauthorized functions, and then hide all traces of its existence.
   Answer: rootkit

Quick Quiz

4. A(n) ______ is a computer program or a part of a program that lies dormant until it is triggered by a specific logical event, such as a certain date reached on the system calendar or a drop below a previous level of a person's rank in an organization.

   Answer:

Quick Quiz

4. A(n) ______ is a computer program or a part of a program that lies dormant until it is triggered by a specific logical event, such as a certain date reached on the system calendar or a drop below a previous level of a person's rank in an organization.

   Answer: logic bomb

Quick Quiz

4. A(n) ______ is a computer program or a part of a program that lies dormant until it is triggered by a specific logical event, such as a certain date reached on the system calendar or a drop below a previous level of a person's rank in an organization.
   Answer: logic bomb

5. A type of malware that gives access to a computer, program, or service that circumvents any normal security protections and allows an attacker to bypass security settings is known as a(n) ______.
   Answer:

Quick Quiz

4. A(n) ______ is a computer program or a part of a program that lies dormant until it is triggered by a specific logical event, such as a certain date reached on the system calendar or a drop below a previous level of a person's rank in an organization.
   Answer: logic bomb

5. A type of malware that gives access to a computer, program, or service that circumvents any normal security protections and allows an attacker to bypass security settings is known as a(n) ______.
   Answer: backdoor

Social Engineering Attacks

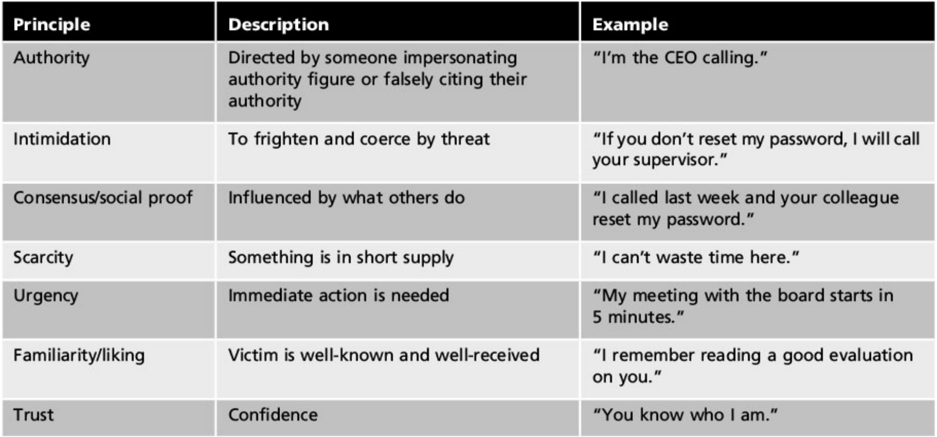
- Social engineering – Means of gathering information from individuals by relying on their weaknesses
- Social engineering attacks can involve:
  - Psychological approaches
  - Physical procedures

Social Engineering Attacks

Psychological Approaches

- Psychology – The mental and emotional approach in social engineering attack
- Social engineering psychological attacks relies on attacker's clever manipulation of human nature to persuade victim to:
  - Provide information
  - Take actions
- Several basic *principles* or *reasons* make psychological social engineering effective (see Table 2-6)

Social Engineering Attacks



Principle	Description	Example
Authority	Directed by someone impersonating authority figure or falsely citing their authority	“I’m the CEO calling.”
Intimidation	To frighten and coerce by threat	“If you don’t reset my password, I will call your supervisor.”
Consensus/social proof	Influenced by what others do	“I called last week and your colleague reset my password.”
Scarcity	Something is in short supply	“I can’t waste time here.”
Urgency	Immediate action is needed	“My meeting with the board starts in 5 minutes.”
Familiarity/liking	Victim is well-known and well-received	“I remember reading a good evaluation on you.”
Trust	Confidence	“You know who I am.”

Table 2-6 Social engineering effectiveness

Social Engineering Attacks

Psychological Approaches

- Attacker will ask for only small amounts of information, often from several different victims
- Request needs to be believable
- Attacker *pushes the envelope* to get information before victim suspects anything
- Flattery and flirtation often used
- Attacker may smile and ask for help

Social Engineering Attacks

Psychological Approaches

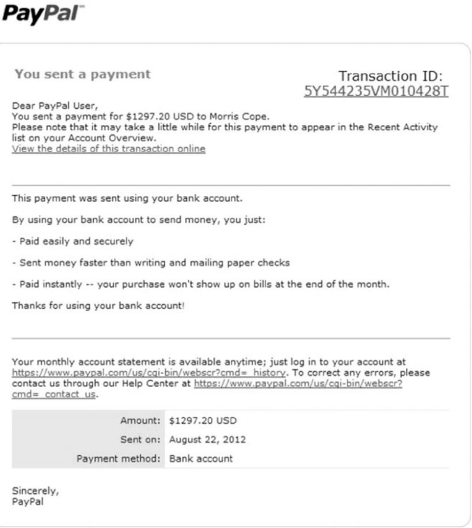
- Impersonation – Masquerade as a real or fictitious character and then play out the role of that person on a victim
- Common roles impersonated:
  - Repairperson
  - IT support
  - Manager
  - Trusted third party
  - Fellow employee

Social Engineering Attacks

Psychological Approaches

- Phishing – Sending email or display web announcement claiming to be from legitimate source
- May contain legitimate logos and wording
- Tries to trick user into giving private information
  - Passwords
  - Credit card numbers
  - Social Security numbers
  - Bank account numbers

Social Engineering Attacks



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 2-8 Phishing email message

Source: Email sent to Dr. Mark Revels

Social Engineering Attacks

Common Phishing Features – Psychological Approaches

- Deceptive web links – Use variations of a legitimate address (e.g. www.ebay_secure.com, www.e–bay.com, www.e-baynet.com)
- Logos – Include logo of vendor to make request look genuine
- Urgent request – Include instructions requiring immediate action or else something serious will occur (user's account will be unavailable or a large amount of money will be deducted from their account)

Social Engineering Attacks

Phishing Variations – Psychological Approaches

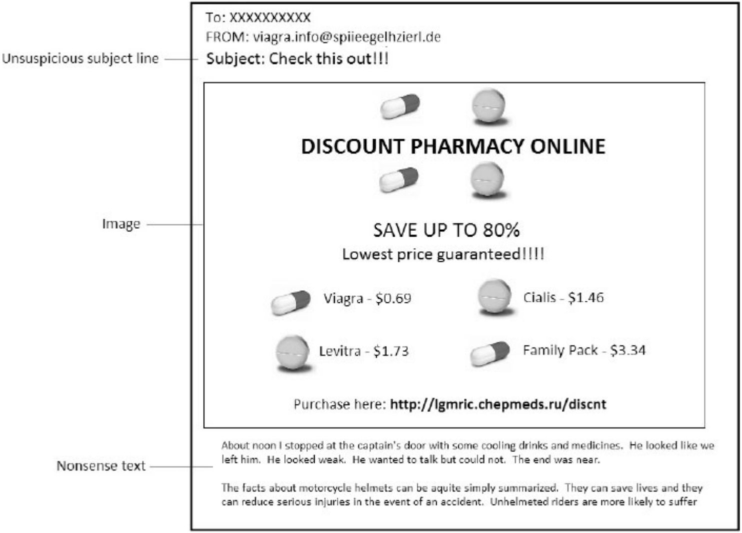
- Pharming – Automatically redirects user to fraudulent web site
- Spear phishing – Email messages target specific users
- Whaling – Going after the *big fish* by targeting wealthy individuals
- Vishing (voice phishing) – Attacker calls victim with recorded message with callback number, but number is actually to attacker

Social Engineering Attacks

Psychological Approaches

- Spam – Unsolicited email
- One of primary vehicles for distribution of malware
- Sending spam is lucrative business
- Spim – Targets instant messaging users
- Image spam:
  - Uses graphical images of text
  - Circumvents text-based filters
  - Often contains nonsense text

Social Engineering Attacks



Unsuspicious subject line

Image

Nonsense text

To: XXXXXXXXXX
FROM: viagra.info@spiieegelhzierl.de
Subject: Check this out!!!

DISCOUNT PHARMACY ONLINE

SAVE UP TO 80%

Lowest price guaranteed!!!!

Viagra - $0.69	Cialis - $1.46
Levitra - $1.73	Family Pack - $3.34

Purchase here: **http://lgmric.chepmeds.ru/discnt**

About noon I stopped at the captain's door with some cooling drinks and medicines. He looked like we left him. He looked weak. He wanted to talk but could not. The end was near.

The facts about motorcycle helmets can be aquite simply summarized. They can save lives and they can reduce serious injuries in the event of an accident. Unhelmeted riders are more likely to suffer

Figure 2-9 Image spam

Social Engineering Attacks

Psychological Approaches

- Hoaxes – False warning or claim
- May be first step in an attack
- Hoax purports that *deadly virus* circulating through the Internet and that the recipient should:
    - Erase specific files
    - Change security configurations
    - Forward message to other users
- However, changing configurations allow an attacker to compromise the system

Social Engineering Attacks

Psychological Approaches

- Typo squatting (URL hijacking) – Attacker registers fake look-alike site to which user is automatically directed when makes a typing error when entering URL (Uniform Resource Locator) address in a web browser (e.g. goggle.com or google.net instead of google.com)
- Site may contain:
  - Visitor survey that promises a chance to win prizes (but the attacker actually captures the entered email addresses to sell to spammers)
  - Ads (for which the attacker receives money for traffic generated to the site)

Social Engineering Attacks

Psychological Approaches

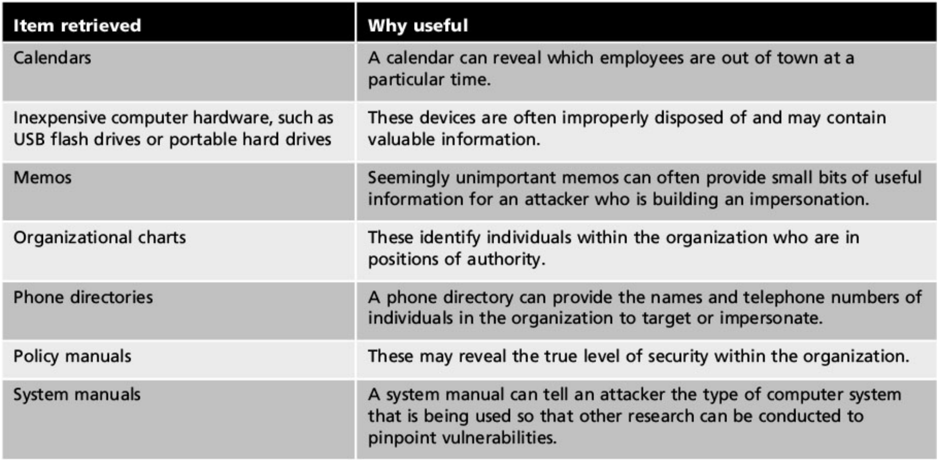
- Similar types of animals congregate around a pool of water for refreshment
- Watering hole attack – Directed toward smaller group of specific individuals, such as the major executives working for a manufacturing company
- These executives all tend to visit a common website, so attacker focuses on compromising that site

Social Engineering Attacks

Physical Procedures

- Just as some social engineering attacks rely on psychological manipulation, other attacks rely on physical acts
- These attacks take advantage of user actions that can result in compromised security
- Two (2) of the most common physical prcedures are:
  1. Dumpster Diving – Digging through trash to find useful information
  2. Tailgating

Social Engineering Attacks



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 portable hard drives	These devices are often improperly disposed of and may 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	A phone directory 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	A system manual can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities.

Table 2-7 **Dumpster diving items and their usefulness**

Social Engineering Attacks

- Tailgating – Following an authorized person entering through a door
- Methods of tailgating:
    - Tailgater calls *please hold the door*
    - Waits outside door and enters when authorized employee leaves
    - Employee conspires with unauthorized person to walk together through open door (a.k.a. *piggybacking*)
- Shoulder surfing – Casually observing user entering keypad code

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as _______ procedures.
   Answer:

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as _______ procedures.
   Answer: physical

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as _______ procedures.
   Answer: physical

2. _______ is a social engineering approach where a user masquerades as a real or fictitious character and then plays out the role of that person on a victim.
   Answer:

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as ______ procedures.
   Answer: physical

2. ______ is a social engineering approach where a user masquerades as a real or fictitious character and then plays out the role of that person on a victim.
   Answer: impersonation

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as ______ procedures.
   Answer: physical

2. ______ is a social engineering approach where a user masquerades as a real or fictitious character and then plays out the role of that person on a victim.
   Answer: impersonation

3. Which type of phishing attack automatically redirects the user to a fake web site?
   Answer:

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as _______ procedures.
   Answer: physical

2. _______ is a social engineering approach where a user masquerades as a real or fictitious character and then plays out the role of that person on a victim.
   Answer: impersonation

3. Which type of phishing attack automatically redirects the user to a fake web site?
   Answer: pharming

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as ______ procedures.
   Answer: physical

2. ______ is a social engineering approach where a user masquerades as a real or fictitious character and then plays out the role of that person on a victim.
   Answer: impersonation

3. Which type of phishing attack automatically redirects the user to a fake web site?
   Answer: pharming

4. ______ is a form of tailgating that involves the tailgater colluding with an authorized person.
   Answer:

Quick Quiz

1. Social engineering attacks can involve psychological approaches as well as _______ procedures.
   Answer: physical

2. _______ is a social engineering approach where a user masquerades as a real or fictitious character and then plays out the role of that person on a victim.
   Answer: impersonation

3. Which type of phishing attack automatically redirects the user to a fake web site?
   Answer: pharming

4. _______ is a form of tailgating that involves the tailgater colluding with an authorized person.
   Answer: Piggybacking