Malware

- Short for ***mal****icious soft****ware.***
- A is software used or created to **disrupt computer operation, gather sensitive information, or gain access to private computer systems**.
- It can appear in the form of code, scripts, active content, and other software.
- 'Malware' is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software

Usage of Malware

- Many early infectious programs, including the first Internet Worm, were written as experiments or pranks.
- Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others.
- Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general.
- However, malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on.

Types of Malware

- Viruses
- Trojan horses
- Worms
- Spyware
- Zombie
- Phishing
- Spam
- Adware
- Ransomware

Types of Malware

Viruses

- A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- Viruses can also replicate themselves.
- All computer viruses are manmade.
- Viruses copy themselves to other disks to spread to other computers.
- They can be merely annoying or they can be vastly destructive to your files.

Types of Malware

Viruses

- Examples of computer viruses are:
  - Macro virus
  - Boot virus
  - Logic Bomb virus
  - Directory virus
  - Resident virus

Types of Malware

Trojan Horses

- A Trojan Horse program has the appearance of having a useful and desired function.
- A Trojan Horse neither replicates nor copies itself, but causes damage or compromises the security of the computer.
- A Trojan Horse must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort.
- These are often used to capture your logins and passwords.

Types of Malware

Example of Trojan Horses

- Remote access Trojans (RATs)
- Backdoor Trojans (backdoors)
- IRC Trojans (IRCbots)
- Keylogging Trojans.

Types of Malware

Worms

- A computer worm is a self-replicating computer program.
- It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.
- It does not need to attach itself to an existing program.

Types of Malware

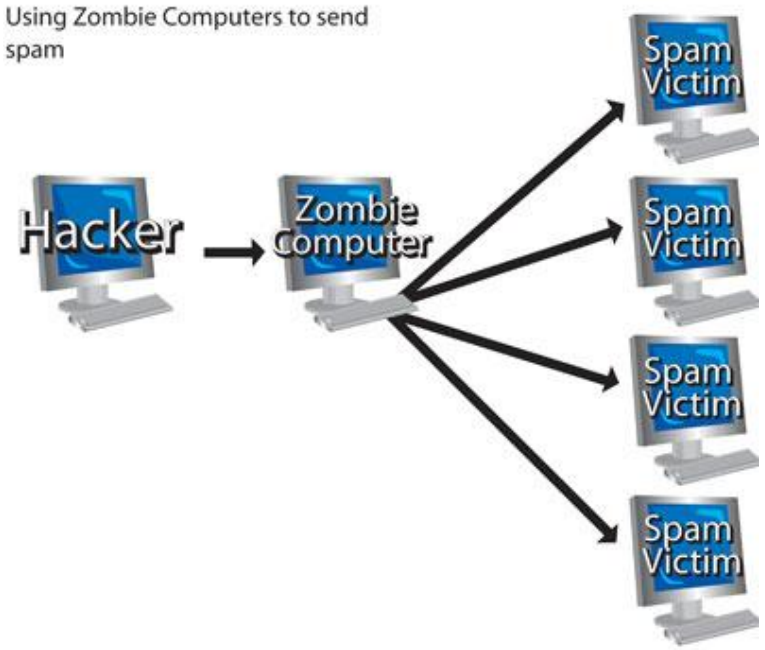
Spyware

- **Spyware** is a type of malware installed on computers that collects information about users without their knowledge.
- The presence of spyware is typically hidden from the user and can be difficult to detect.
- Spyware programs lurk on your computer to steal important information, like your passwords and logins and other personal identification information and then send it off to someone else.

Types of Malware

Zombie

- **Zombie** programs take control of your computer and use it and its Internet connection to attack other computers or networks or to perform other criminal activities.



Types of Malware

Phishing

- Phishing (pronounced like the word 'fishing') is a message that tries to trick you into providing information like your social security number or bank account information or logon and password for a web site.
- The message may claim that if you do not click on the link in the message and log onto a financial web site that your account will be blocked, or some other disaster.

Types of Malware

Phishing

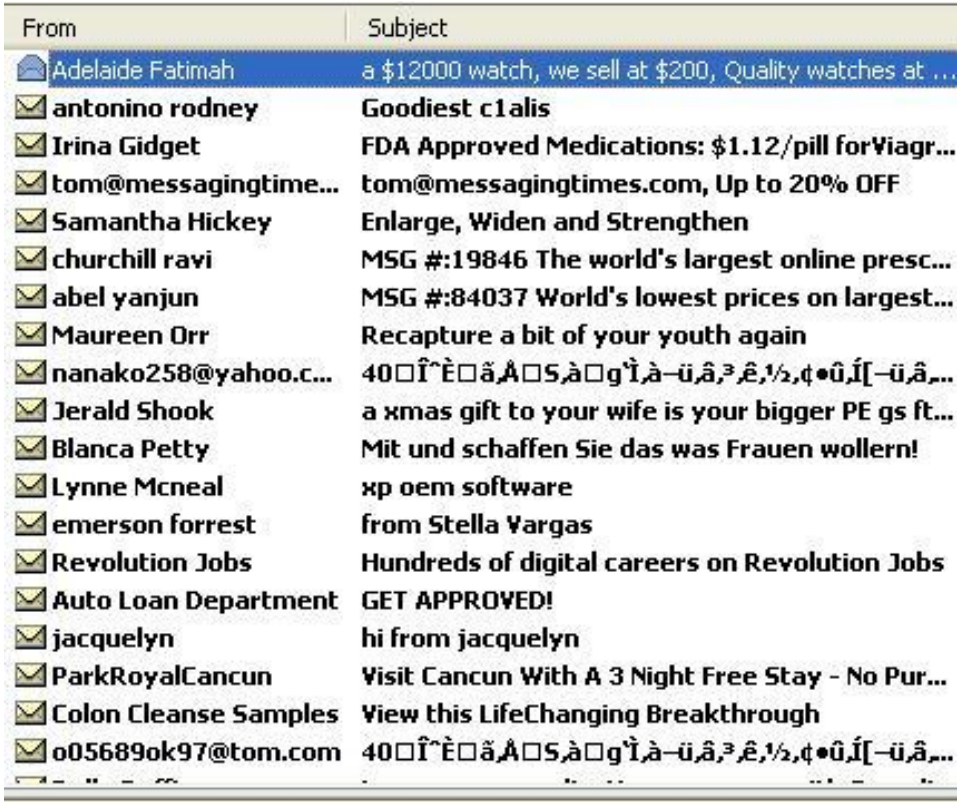
Types of Malware

Spam

- Spam is email that you did not request and do not want.
- One person's spam is another's useful newsletter or sale ad.
- Spam is a common way to spread viruses, trojans, and the like.

Types of Malware

Spam



From	Subject
Adelaide Fatimah	a $12000 watch, we sell at $200, Quality watches at ...
antonino rodney	Goodiest c1alis
Irina Gidget	FDA Approved Medications: $1.12/pill forViagr...
tom@messagingtime...	tom@messagingtimes.com, Up to 20% OFF
Samantha Hickey	Enlarge, Widen and Strengthen
churchill ravi	MSG #:19846 The world's largest online presc...
abel yanjun	MSG #:84037 World's lowest prices on largest...
Maureen Orr	Recapture a bit of your youth again
nanako258@yahoo.c...	40□Î^È□ã,Å□S,à□g'Ì,à–ü,â,³,ê,½,¢•û,Í[–ü,â,...
Jerald Shook	a xmas gift to your wife is your bigger PE gs ft...
Blanca Petty	Mit und schaffen Sie das was Frauen wollern!
Lynne Mcneal	xp oem software
emerson forrest	from Stella Vargas
Revolution Jobs	Hundreds of digital careers on Revolution Jobs
Auto Loan Department	GET APPROVED!
jacquelyn	hi from jacquelyn
ParkRoyalCancun	Visit Cancun With A 3 Night Free Stay - No Pur...
Colon Cleanse Samples	View this LifeChanging Breakthrough
o05689ok97@tom.com	40□Î^È□ã,Å□S,à□g'Ì,à–ü,â,³,ê,½,¢•û,Í[–ü,â,...

Types of Malware

Adware

- Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.
- Common examples of adware include pop-up ads on websites and advertisements that are displayed by software.
- Often times software and applications offer “free” versions that come bundled with adware.

Types of Malware

Adware

Types of Malware

Ransomware

- Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom.
- The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer.

How Malware Spreads?

- Malware is a program that must be triggered or somehow executed before it can infect your computer system and spread to others.
- Here are some examples on how malware is distributed:
  a) Social network
  b) Pirated software
  c) Removable media
  d) Emails
  e) Websites

Damages

1. Data Loss

- Many viruses and Trojans will attempt to delete files or wipe hard drives when activated, but even if you catch the infection early, you may have to delete infected files.

Damages

2. Account Theft

- Many types of malware include keylogger functions, designed to steal accounts and passwords from their targets.
- This can give the malware author access to any of the user's online accounts, including email servers from which the hacker can launch new attacks.

Damages

3. Botnets

- Many types of malware also subvert control over the user's computer, turning it into a "bot" or "zombie."
- Hackers build networks of these commandeered computers, using their combined processing power for tasks like cracking password files or sending out bulk emails.

Damages

4. Financial Losses

- If a hacker gains access to a credit card or bank account via a keylogger, he can then use that information to run up charges or drain the account.
- Given the popularity of online banking and bill payment services, a hacker who manages to secrete a keylogger on a user's system for a full month may gain access to the user's entire financial portfolio, allowing him to do as much damage as possible in a single attack.

How Can You Protect Your Computer?

- Install protection software.
- Practice caution when working with files from unknown or questionable sources.
- Do not open e-mail if you do not recognize the sender.
- Download files only from reputable Internet sites.
- Install firewall.
- Scan your hard drive for viruses monthly.

Symptoms

- Increased CPU usage
- Slow computer or web browser speeds
- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)

Symptoms

- Strange computer behavior
- Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send)
- There seems to be a lot of network activity when you are not using the network
- The available memory on your computer is lower than it should be
- Programs or files appear or disappear without your knowledge
- File names are changed

Anti-Malware Program

- Anti-Malware program is used to prevent, detect, and remove computer viruses, worms, trojan horses and any other type of malware.
- Examples of Anti-Malware program:
  - Antivirus program
  - Anti-spyware program
  - Anti-spam program
  - Firewall

Antivirus Program

- “Antivirus" is protective software designed to defend your computer against malicious software.
- In order to be an effective defense, the antivirus software needs to run in the background at all times, and should be kept updated so it recognizes new versions of malicious software.

Examples of Antivirus Program

- Norton Antivirus
- AVG
- Kaspersky
- Avast!
- PC-Cilin
- McAffee
- Avira

Anti-Spyware Program

- Anti-spyware program is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.
- Examples of Anti-spyware program:
  - Spyware Doctor
  - AVG Anti-spyware
  - STOPzilla
  - Spysweeper

Anti-Spam Program

- Anti-spam software tries to identify useless or dangerous messages for you.

Firewall

- A firewall blocks attempts to access your files over a network or internet connection.
- That will block incoming attacks.
- Your computer can become infected through shared disks or even from another computer on the network.
- So you need to monitor what your computer is putting out over the network or internet also.