

# Week 5: Attacks: Malicious Software

Ayman El Hajjar

6COSC002W - Security and Forensics

Email: [a.elhajjar@westminster.ac.uk](mailto:a.elhajjar@westminster.ac.uk)

Twitter: [@azelhajjar](https://twitter.com/azelhajjar)

15 February 2020



University of Westminster

# Session Overview

- 1 Malicious Attack
- 2 Malicious Software
- 3 Threats & Countermeasures

# Malicious Code and Activity

- Malicious software (malware)
  - Any program that carries out actions that you do not intend
- Malicious code attacks all three information security properties:
  - Confidentiality: Malware can disclose your organization's private information
  - Integrity: Malware can modify database records, either immediately or over a period of time
  - Availability: Malware can erase or overwrite files or inflict considerable damage to storage media

# Characteristics, Architecture, and Operations of Malicious Software

- An attacker gains administrative control of a system and uses commands to inflict harm
- An attacker sends commands directly to a system; the system interprets and executes them
- An attacker uses software programs that harm a system or that make the data unusable
- An attacker uses legitimate remote administration tools and security probes to identify and exploit security vulnerabilities on a network

# The Main Types of Malware

- Viruses
- Spam
- Worms
- Trojan horses
- Logic bombs
- Active content vulnerabilities
- Malicious add-ons
- Injection
- Botnets
- Denial of service attacks
- Spyware
- Adware
- Phishing
- Keystroke loggers
- Hoaxes and myths
- Homepage hijacking
- Webpage defacements

# What Is Malicious Software?

Software that:

Causes damage

Escalates security privileges

Divulges private data

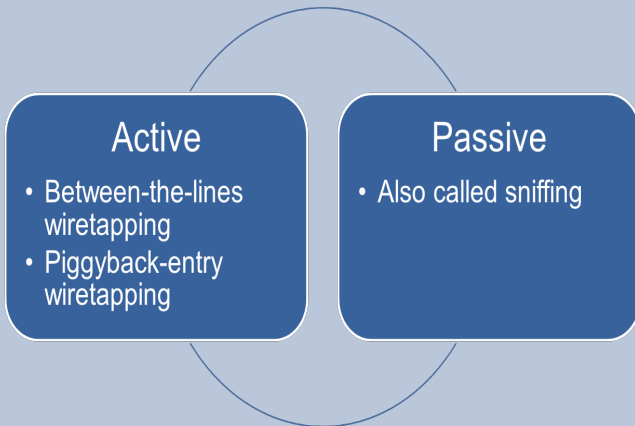
Modifies or deletes data

# Spyware

Type of malware that specifically threatens the confidentiality of information

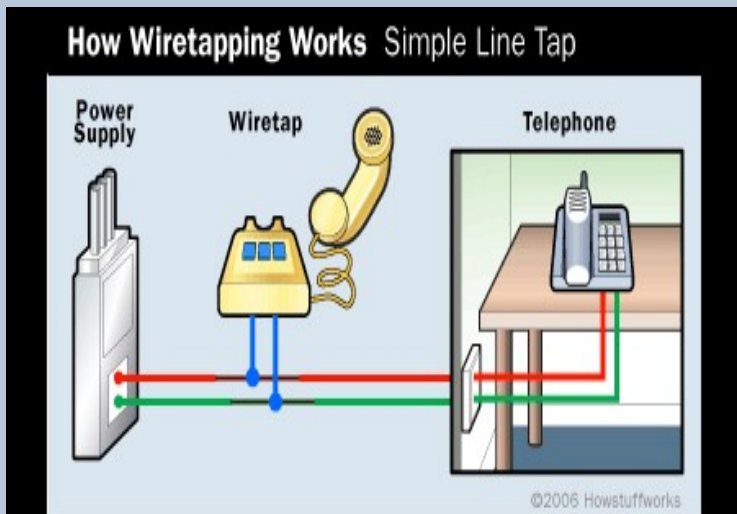
- Monitors keystrokes
- Scans files on the hard drive
- Snoops other applications
- Installs other spyware programs
- Reads cookies
- Changes default homepage on the web browser

# Wiretapping

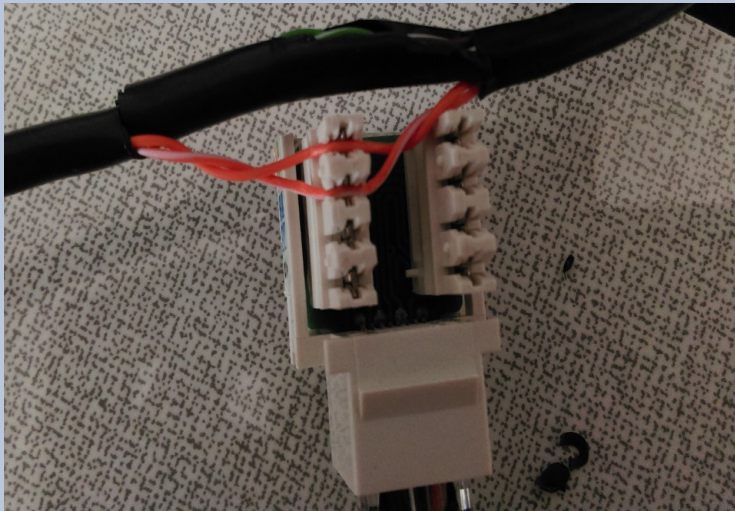




# Wiretapping Telephone



# Wiretapping Networks



# Backdoors

- Hidden access included by developers
- Attackers can use them to gain access
- Data Modifications
- Data that is:
  - Purposely or accidentally modified
  - Incomplete
  - Truncated

# Viruses

## System infectors

- Target computer hardware and software startup functions

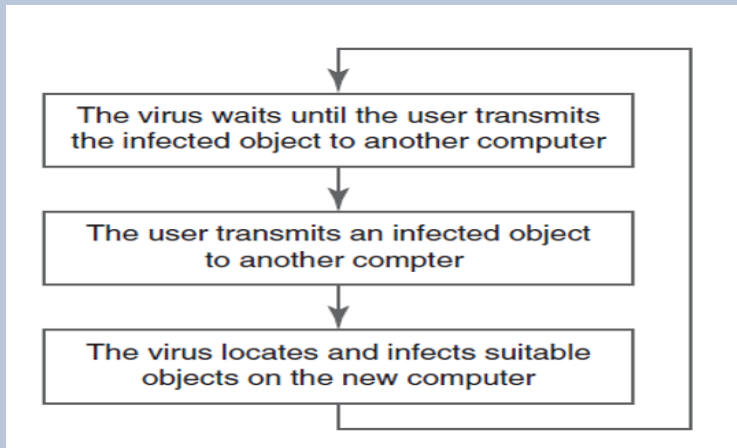
## File infectors

- Attack and modify executable programs (COM, EXE, SYS, and DLL files in Microsoft Windows)

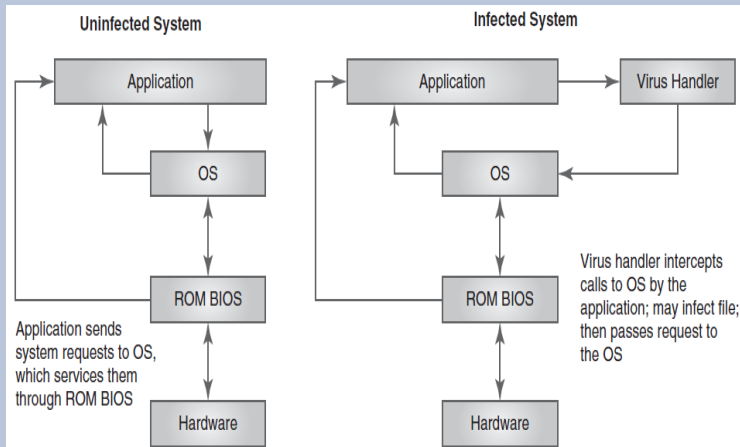
## Data infectors

- (Also called macro infectors) Attack document files containing embedded macro programming capabilities

# Typical Life Cycle of a Computer Virus



# How a System Infector Virus Works



# Rootkit

Modifies or replaces one or more existing programs to hide traces of attacks

Many different types of rootkits

Conceals its existence once installed

Is difficult to detect and remove

# Rootkits

Type of malware that modifies or replaces one or more existing programs to hide the fact that a computer has been compromised

Modify parts of the operating system to conceal traces of their presence

Provide attackers with access to compromised computers and easy access to launching additional attacks

Difficult to detect and remove



# Ransomware

Attempts to generate funds directly from a computer user

Attacks a computer and limits the user's ability to access the computer's data

Encrypts important files or even the entire disk and makes them inaccessible

One of the first ransomware programs was Crypt0L0cker

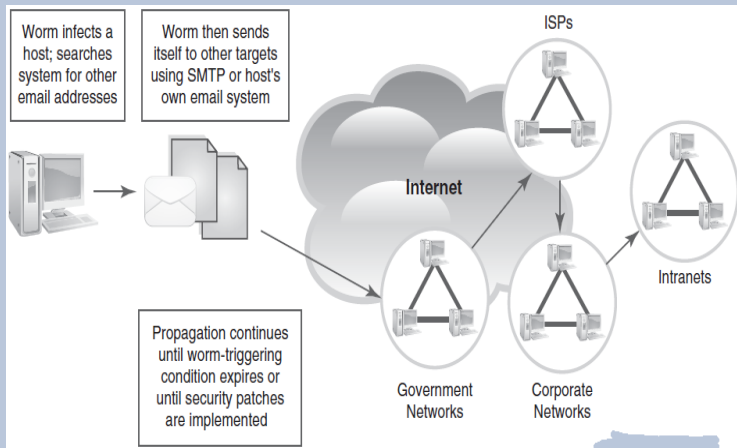
# Spam

- Consumes computing resources bandwidth and CPU time
- Diverts IT personnel from activities more critical to network security
- Is a potential carrier of malicious code
- Compromises intermediate systems to facilitate remailing services
- Opt-out (unsubscribe) features in spam messages can represent a new form of reconnaissance attack to acquire legitimate target addresses

# Worms

- Designed to propagate from one host machine to another using the host's own network communications protocols
- Unlike viruses, do not require a host program to survive and replicate
- The term "worm" stems from the fact that worms are programs with segments, working on different computers, all communicating over a network

## Worms (cont.)



# Trojan Horses

Largest class of malware

Any program that masquerades as a useful program while hiding its malicious intent

Relies on social engineering to spread and operate

Spreads through email messages, website downloads, social networking sites, and automated distribution agents (bots)

# Logic Bombs

Programs that execute a malicious function of some kind when they detect certain conditions

Typically originate with organization insiders because people inside an organization generally have more detailed knowledge of the IT infrastructure than outsiders

# Active Content Vulnerabilities

- Active content
  - Refers to dynamic objects that do something when the user opens a webpage (ActiveX, Java, JavaScript, VBScript, macros, browser plugins, PDF files, and other scripting languages)
  - Has potential weaknesses that malware can exploit
- Active content threats are considered mobile code because these programs run on a wide variety of computer platforms
- Users download bits of mobile code, which gain access to the hard disk and do things like fill up desktop with infected file icons

# Malicious Add-Ons

Add-ons are companion programs that extend the web browser; can decrease security

Malicious add-ons are browser add-ons that contain some type of malware that, once installed, perform malicious actions

Only install browser add-ons from sources you trust



# Injection

Cross-site scripting (XSS)

SQL injection

LDAP injection

XML injection

Command injection

# Spyware

Any unsolicited background process that installs itself on a user's computer and collects information about the user's browsing habits and website activities

Affects privacy and confidentiality

Spyware cookies are cookies that share information across sites

Some cookies are persistent and are stored on a hard drive indefinitely without user permission

# Adware

Triggers nuisances  
such as popup ads  
and banners when  
user visits certain  
websites

Affects productivity  
and may combine  
with active  
background  
activities

Collects and tracks  
information about  
application, website,  
and Internet activity

# Phishing

Tricks users into providing logon information on what appears to be a legitimate website but is actually a website set up by an attacker to obtain this information

## Spear-phishing

- Attacker supplies information about victim that appears to come from a legitimate company

## Pharming


- The use of social engineering to obtain access credentials such as usernames and passwords

# Keystroke Loggers


Capture keystrokes  
or user entries and  
forwards information  
to attacker

Enable the attacker to  
capture logon  
information, banking  
information, and other  
sensitive data

# Homepage Hijacking



Exploiting a browser vulnerability to reset the homepage

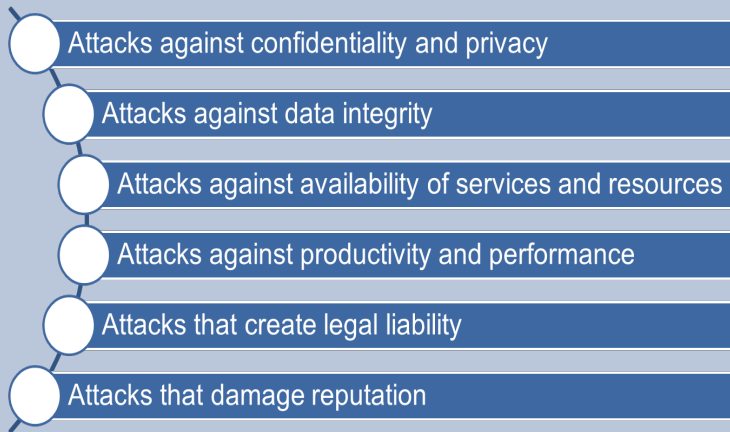


Covertly installing a browser helper object (BHO) Trojan program

# Webpage Defacements

- Someone gaining unauthorized access to a web server and altering the index page of a site on the server
- The attacker replaces the original pages on the site with altered versions

# Threats to Business Organizations





# Internal Threats from Employees: Unsafe Computing Practices

Exchange of untrusted disks or other media among systems

Installation of unauthorized, unregistered software

Unmonitored download of files from the Internet

Uncontrolled dissemination of email or other messaging application attachments

# What Is a Countermeasure?

## Countermeasures

- Detect vulnerabilities
- Prevent attacks
- Respond to the effects of successful attacks

## Get help from

- Law enforcement agencies
- Forensic experts
- Security consultants
- Security incident response teams (SIRTs)

# Countering Malware

- Create a user education program
- Post regular bulletins about malware problems
- Never transfer files from an unknown or untrusted source (unless anti-malware is installed)
- Test new programs or open suspect files on a quarantine computer
- Install anti-malware software, make sure it remains current, and schedule regular malware scans
- Use a secure logon and authentication process

# Attack Prevention Tools and Techniques

- Defense in depth
  - The practice of layering defenses into zones to increase the overall protection level and provide more reaction time to respond to incidents
    - Application defenses
    - Operating system defenses
    - Network infrastructure defenses

# Application Defenses

- Implementing regular antivirus screening on all host systems
- Ensuring that virus definition files are up to date
- Requiring scanning of all removable media
- Installing personal firewall and IDS software on hosts
- Deploying change detection software and integrity checking software
- Maintaining logs
- Implementing email usage controls and ensuring that email attachments are scanned

# Operating System Defenses

- Deploying change detection and integrity checking software and maintaining logs
- Deploying or enabling change detection and integrity checking software on all servers
- Ensuring that operating systems are consistent and have been patched with the latest updates from vendors
- Ensuring that only trusted sources are used when installing and upgrading OS code
- Disabling unnecessary OS services and processes that may pose a security vulnerability

# Network Infrastructure Defenses

- Creating chokepoints in the network
- Using proxy services and bastion hosts to protect critical services
- Using content filtering at chokepoints to screen traffic
- Ensuring that only trusted sources are used when installing and upgrading OS code
- Disabling any unnecessary network services and processes that may pose a security vulnerability
- Maintaining up-to-date IDS signature databases
- Applying security patches to network devices to ensure protection against new threats and reduce vulnerabilities

# Safe Recovery Techniques and Practices

Store OS and data file backup images on external media to ease recovering from potential malware infection



Scan new and replacement media for malware before reinstalling software



Disable network access to systems during restore procedures or upgrades until you have re-enabled or installed protection software or services



# Implementing Effective Software Best Practices

- Adopt an acceptable use policy (AUP) for network services and resources
- Adopt standardized software to better control patches and upgrades and to ensure that you address vulnerabilities
- Consider implementing a compliant security policy such as the ISO/IEC27007- Information security, cybersecurity and privacy protection

# Incident Detection Tools and Techniques

- Antivirus scanning software
- Network monitors and analyzers
- Content/context filtering and logging software
- Honeypots and honeynets

# Summary

- The impact of malicious code and malware on systems and organizations
- Malicious software and countermeasures
- Common attacks and countermeasures
- Social engineering and how to reduce risks
- Tools and techniques to detect and prevent attacks

# References

- The impact of malicious code and malware on systems and organizations
- Malicious software and countermeasures
- Common attacks and countermeasures
- Social engineering and how to reduce risks
- Tools and techniques to detect and prevent attacks