

Malware

Edited by:
Dr. Ahmed Redha

Learning Objective

- Identify common types of malware and the threats they pose.

Key Concepts

- Types of malware
- Malware removal and mitigation
- Trojan behavior, detection, and creation
- Backdoors and covert channels
- Ransomware

Malware Introduction

- Any software that is hostile, intrusive, or annoying in its operation and performs any action or activity without the knowledge or consent of the system's owner.
- Has been adopted by criminals for a wide array of purposes to capture information about the victim or commit other acts.
- Includes viruses, worms, Trojans, spyware, adware, scareware, ransomware, and more.
- Has evolved to steal or destroy information, such as keystroke loggers.

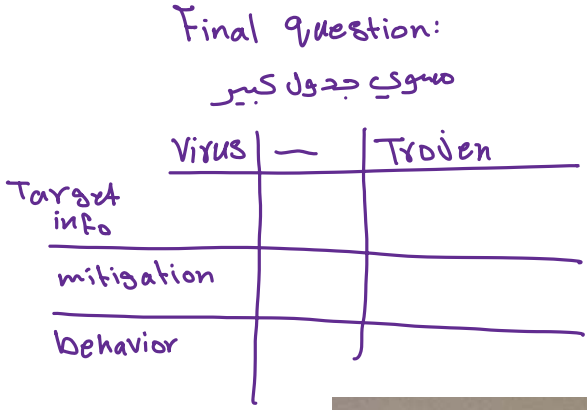
Types of Malware

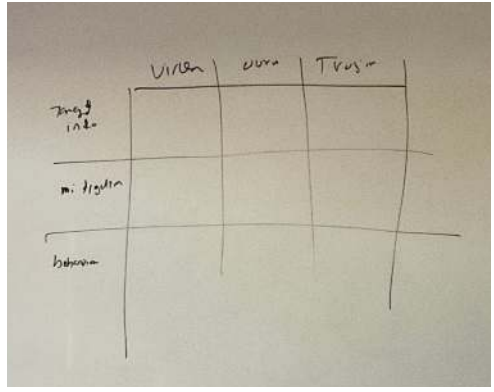


- Viruses
- Worms
- Spyware
- Adware
- Scareware
- Trojans
- Rootkits

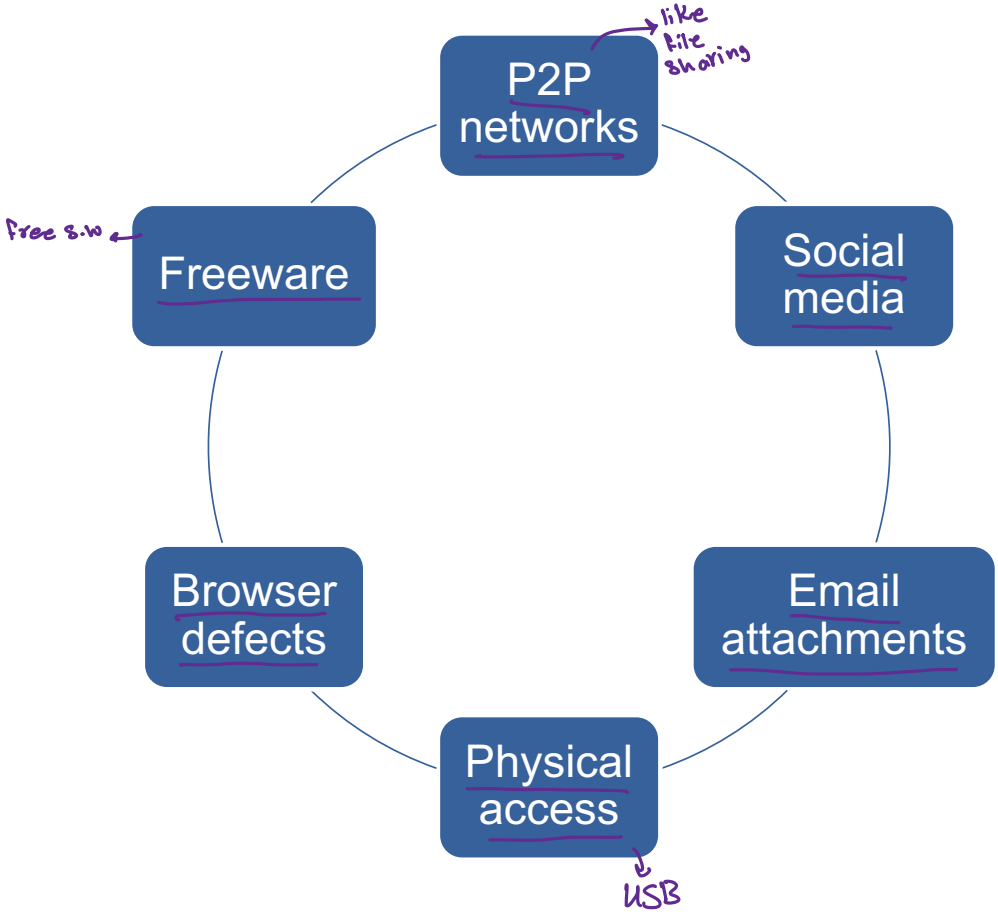
Spyware

- Software designed to collect and report information on a user's activities without the user's knowledge or consent
- Can collect:
  - Browsing habits
  - Keystrokes
  - Software usage
  - General computer usage
  - More



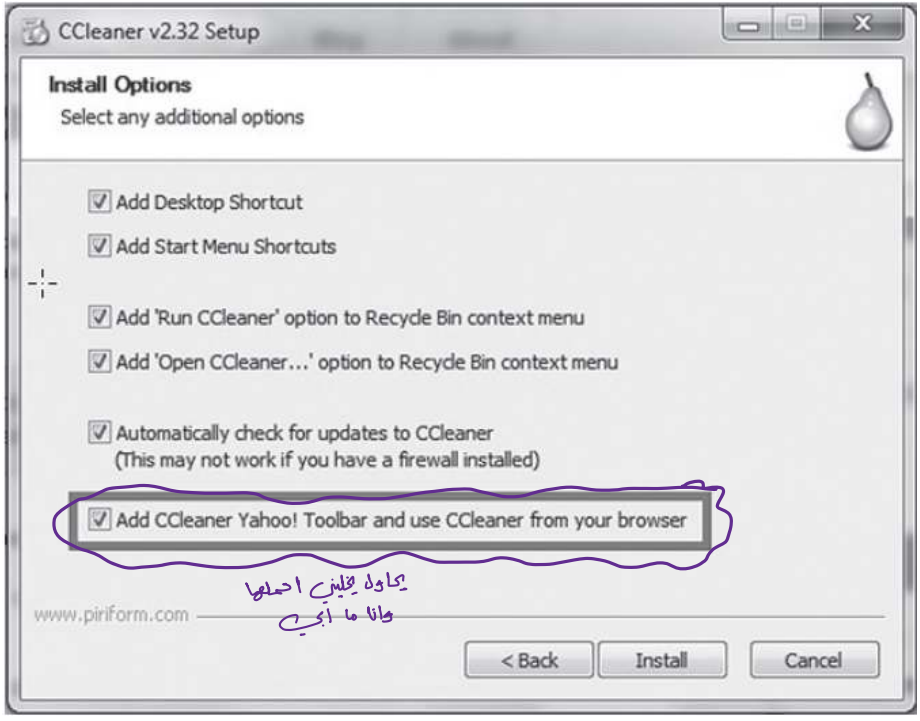


Spyware Methods of Infection



Bundling with Software

freeware



Adware and Scareware

- Adware
  - Software specifically designed to display ads on a user's system in the form of pop-ups or nag screens; often associated with spyware.
- Scareware
  - A type of malware designed to trick victims into purchasing and downloading useless and potentially dangerous software.

Ransomware

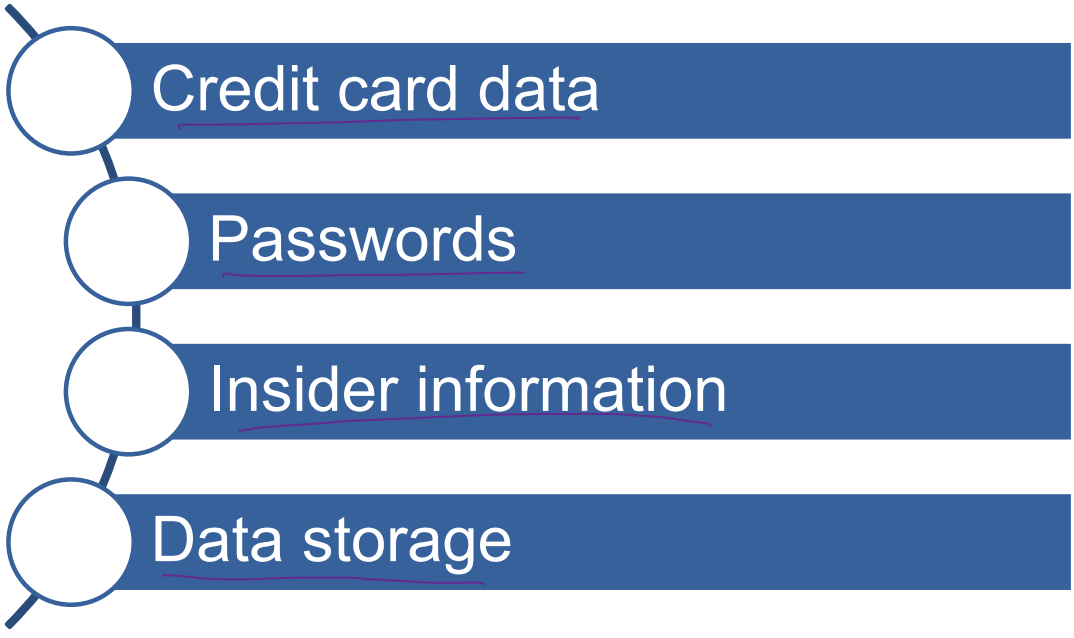
- Designed to hold the user's data hostage.
- Either sends data to the attacker or encrypts large volumes of files and data.
- The victim must send ransom money to the attacker in exchange for the decryption key.

Ransomware (Cont.)

Mitigate

- Defending against ransomware:
  - Install and maintain anti-malware software. Keep it up to date.
  - Apply the latest patches for the operating system and all software.
  - Back up data. (and store it on a device not connected to a network)
  - Restrict files from running in data folders.
  - Don’t use RDP (Remote Desktop).

Malware Targets



Viruses and How They Function

Virus

- Oldest piece of malware software
- Term is frequently used to refer to all types of malware
- A piece of code or software that spreads from system to system by attaching itself to other files
- Virus activates when the file is accessed
- Upon activation, the code carries out the attack or other action the author wishes to execute (destroying or corrupting data, for example)

in exam: coparison

Types of Viruses

- Logic bombs
  - Designed to go off on a specific date or when specific event happens
- Polymorphic viruses
  - Can change its shape to avoid antivirus programs and detection
- Multipartite viruses
  - Infects using multiple attack vectors, including the boot sector and executable files on the hard drive
- Macro viruses
  - Infects and operates using macro language
- Hoaxes
  - Not a true virus but are designed to get the user to take an action even though no infection or threat exists

Virus Prevention

Education

Antivirus/
Anti-malware

Applying
updates

Worms and How They Function

- Self-replicating piece of software that combines the convenience of computer networks with the power of malware.
- Does not require a host program; is self-contained
- Does not require user intervention
- Replicates rapidly
- Consumes bandwidth and resources
- Can transmit information from a victim system.
- Can carry a payload such as a virus.

Stopping Worms

- Patch operating systems
  - Doesn’t protect from a zero-day exploit, in which a hole can be exploited immediately
- Education
  - How to open email safely
  - Don’t respond to phishing messages
- Antivirus
- Firewalls

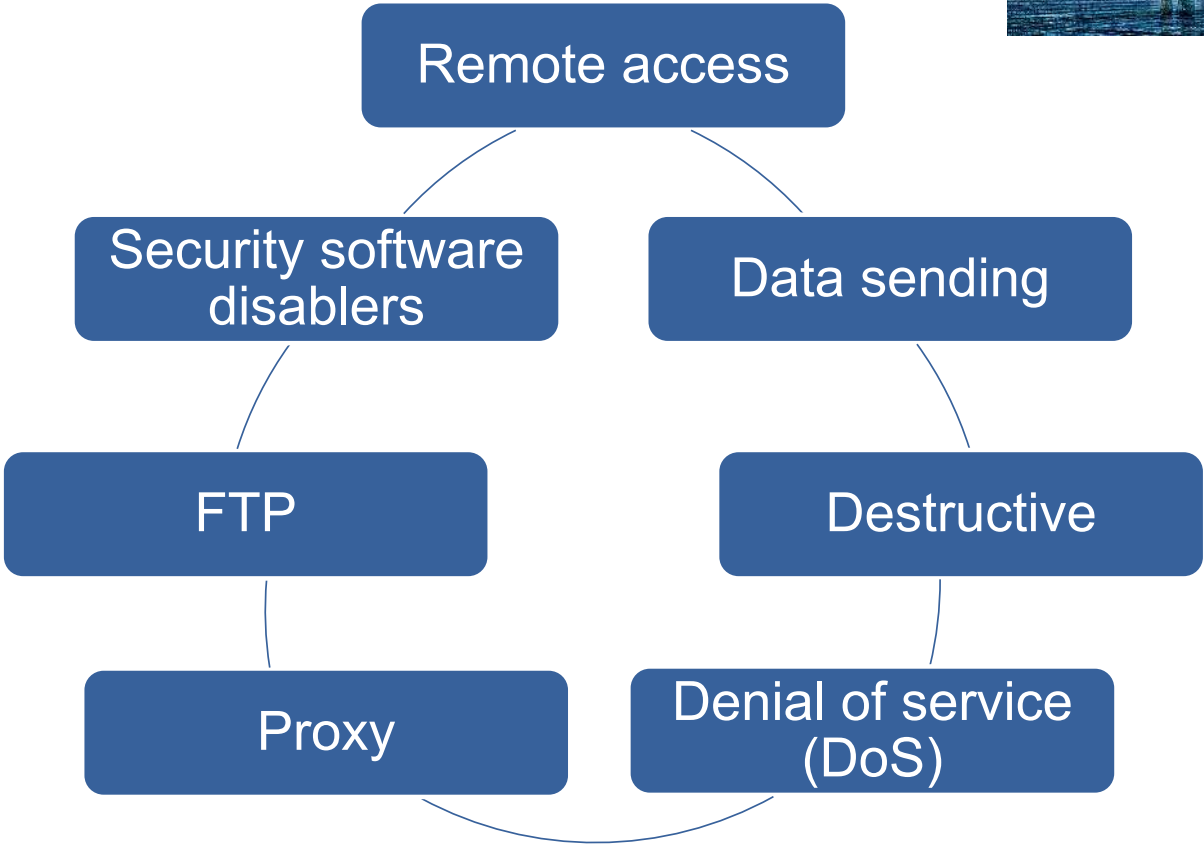


How Is a Worm Different from a Virus?

Virus	Worm
A virus is a file that cannot be spread to other computers unless an infected file is replicated and actually sent to the other computer, whereas a worm does just the opposite.	A worm, after being installed on a system, can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs.
Files such as .com, .exe, or .sys, or a combination of them are corrupted once the virus runs on the system.	A worm typically does not modify any stored programs.
Viruses are a lot harder to get off an infected machine.	As compared to a virus, a worm can be easily removed from the system.
Their spreading options are much less than that of a worm because viruses only infect files on the machine.	They have more spreading options than a virus.

Significance of Trojans: Types





Methods to Get Trojans onto a System

1. A Trojan attaches to another file.
2. The file is retrieved and executed by an unsuspecting victim.
3. The Trojan then typically grants access to the attacker or can do some other action on the attacker's behalf.

Methods to Get Trojans onto a System (Cont.)

- Functions of Trojans:
  - Data theft
  - Installation of software
  - Downloading or uploading of files
  - Modification or deletion of files
  - Installing keystroke loggers
  - Viewing the system user's screen
  - Consuming computer storage space
  - Crashing the victim's system

Targets of Trojans

- Targets
  - Financial data
  - Passwords
  - Insider information
  - Stored data

Known Symptoms of an Infection

- The CD/DVD drawer of a computer opens and closes.
- The computer screen changes, such as flips or inverts.
- Screen settings change by themselves.
- Documents print with no explanation.
- A browser is redirected to a strange or unknown webpage.
- Windows color settings change.
- Screen saver settings change.
- Right and left mouse buttons reverse their functions.
- The mouse pointer disappears.
- The mouse pointer moves in unexplained ways.

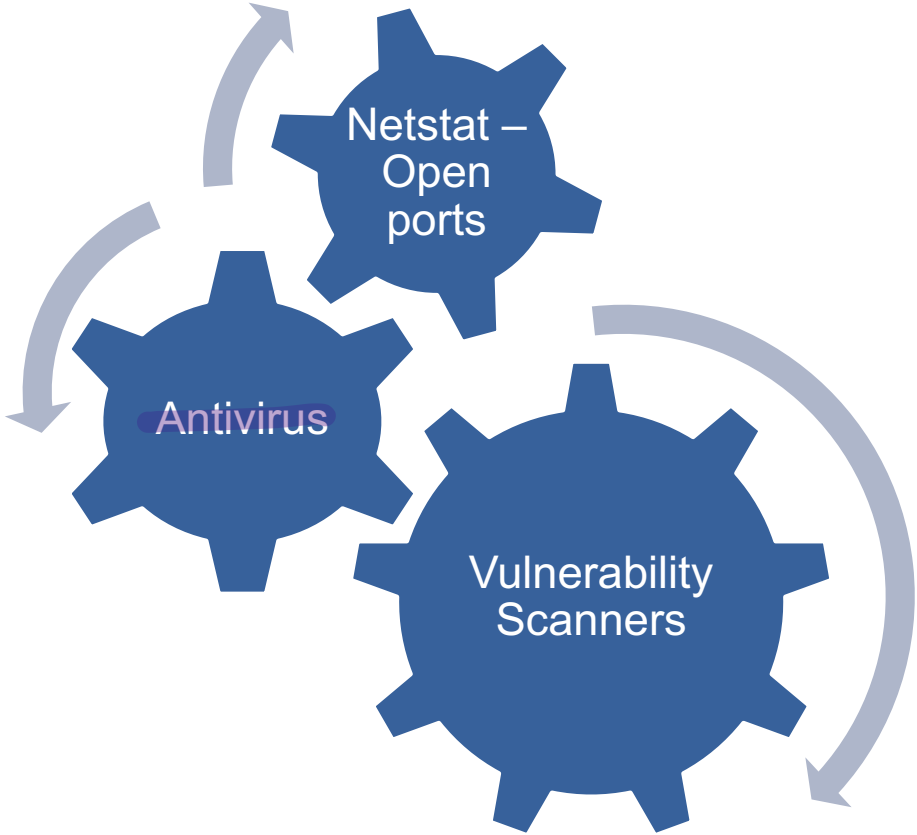
Known Symptoms of an Infection (Cont.)

- The start button disappears.
- Chat boxes appear on the infected system.
- The Internet service provider (ISP) reports that the victim's computer is running port scans.
- People chatting appear to know detailed personal information.
- The system shuts down by itself.
- The taskbar disappears.
- The account passwords are changed.
- Legitimate accounts are accessed without authorization.

Known Symptoms of an Infection (Cont.)

- Unknown purchase statements appear in credit card bills.
- The Ctrl+Alt+Del command stops working.
- Although the computer is rebooted, a message states that there are other users still connected.

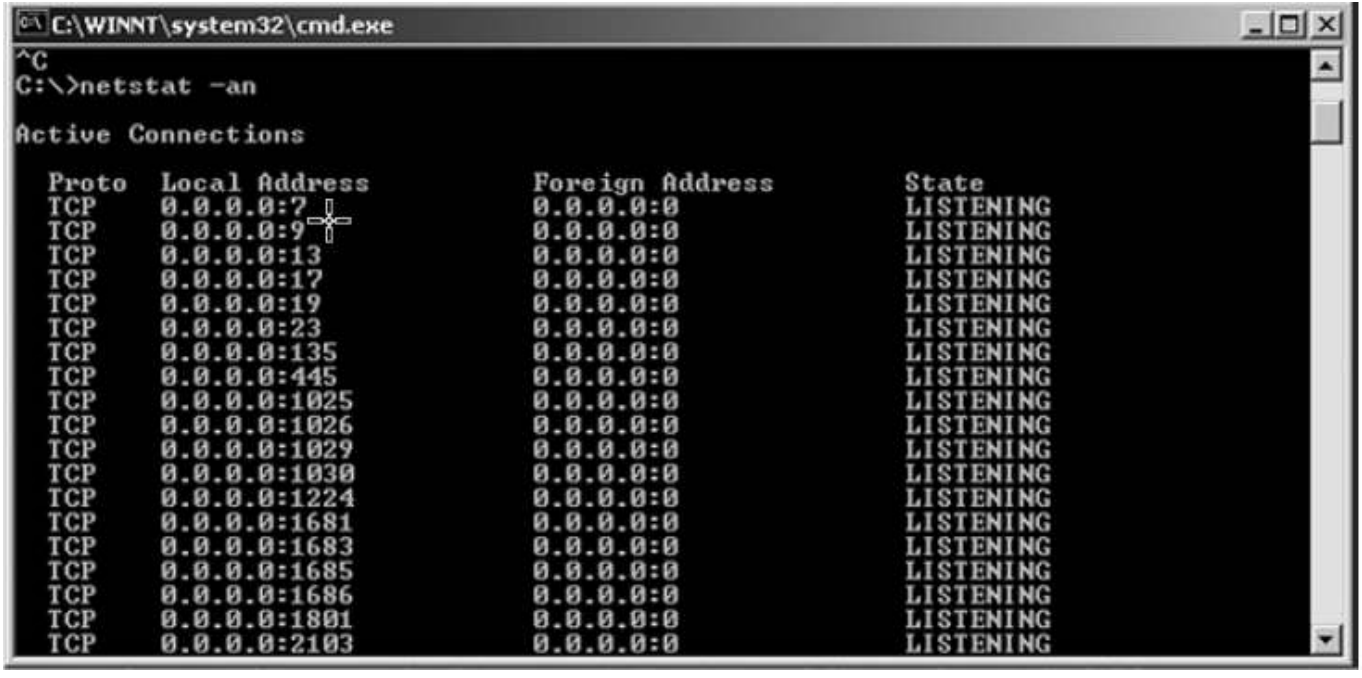
Detection of Trojans and Viruses



Classic Trojans, Ports, and Protocols

TROJAN	PROTOCOL	PORTS
Back Orifice, DeepBO	UDP (User Datagram Protocol)	31337 or 31338
SchoolBus	TCP/UDP (Transmission Control Protocol/User Datagram Protocol)	54320 or 54321
Backdoor	TCP	1999
Deep Throat, The Invasor	TCP	2140 and 3150
Evil FTP, Ugly FTP	TCP	23456
Loki	ICMP (Internet Control Message Protocol)	NA
NetBus, GangBus	TCP	12345 and 12346
Netcat	TCP/UDP	Any
Netmeeting Remote	TCP	49608 and 49609
pcAnywhere	TCP	5631, 5632, or 65301
Reachout	TCP	43188
Remotely Anywhere	TCP	2000 and 2001
Remote	TCP/UDP	135-1139
Whack-a-Mole	TCP	12361 and 12362
NetBus 2 Pro	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423, or 40426
Timbuktu	TCP/UDP	407
VNC	TCP/UDP	5800 or 5801

Results of the `netstat` Command



Trojan Distribution Method: Wrappers

- The attackers merge intended payload with a harmless executable to create a single executable.
- New executable is posted in some location where it is likely to be downloaded.

Wrappers

A wrapper **binds a Trojan executable** with an innocent looking .EXE application such as games or office applications



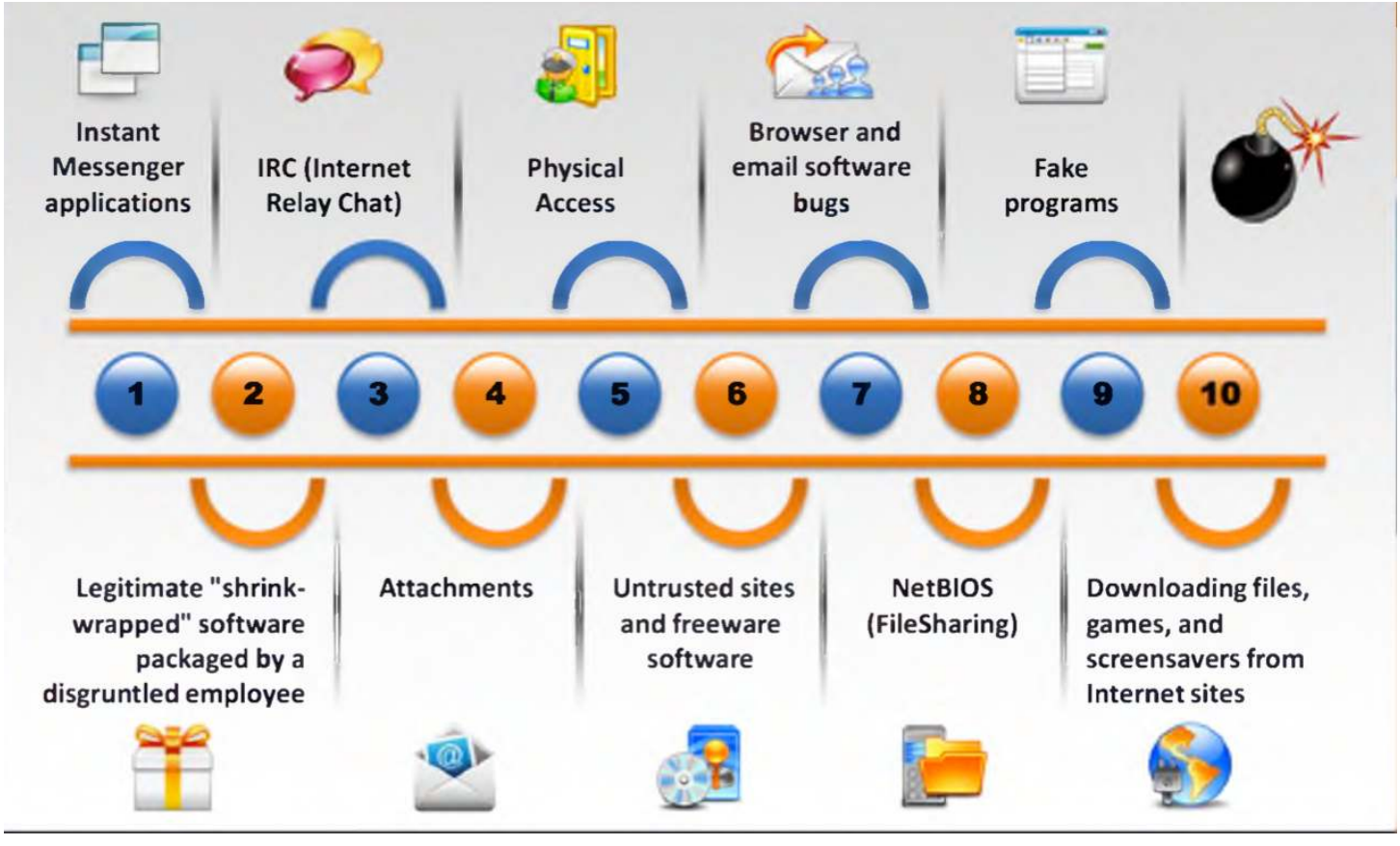
When the user runs the wrapped EXE, it first installs the **Trojan in the background** and then runs the wrapping application in the foreground

The two programs are **wrapped together** into a single file

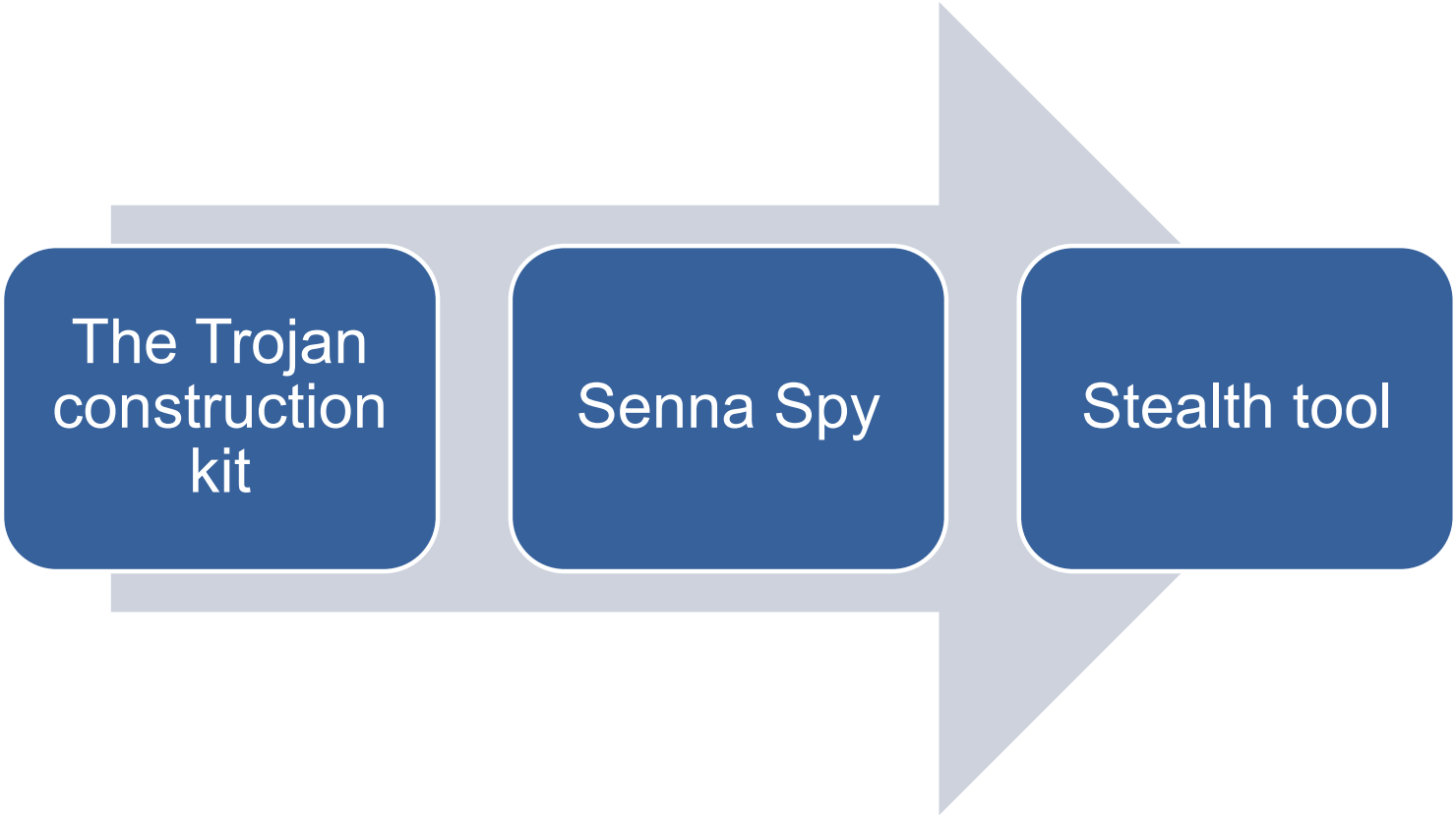


Attackers might send a **birthday greeting** that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen

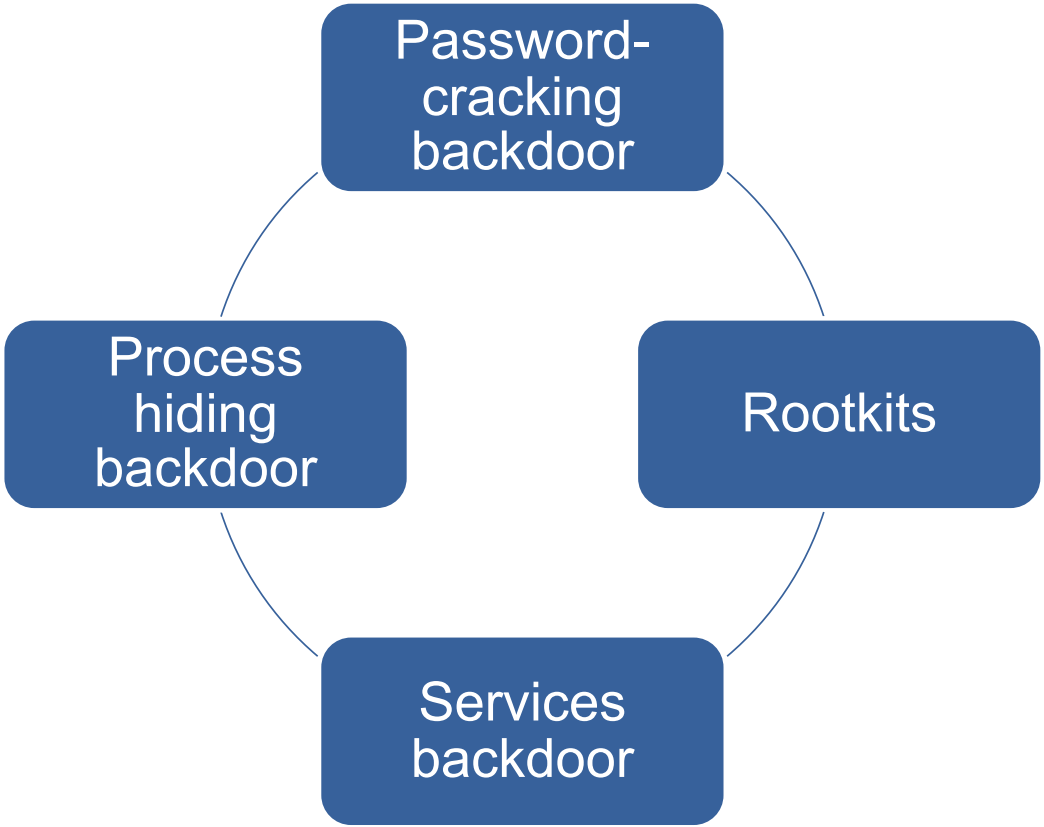
Different ways a Trojan can get into a System



Trojan Construction Kits



Backdoors


Password-cracking backdoor
Rootkits
Services backdoor
Process hiding backdoor

Keystroke Loggers

- Are typically implemented as hardware or software
- Software is installed just like any other Trojan
  - Examples: IKS Software Keylogger and Ghost Keylogger
- Hardware-based keystroke loggers are plugged into a universal serial bus (USB) or PS2 port

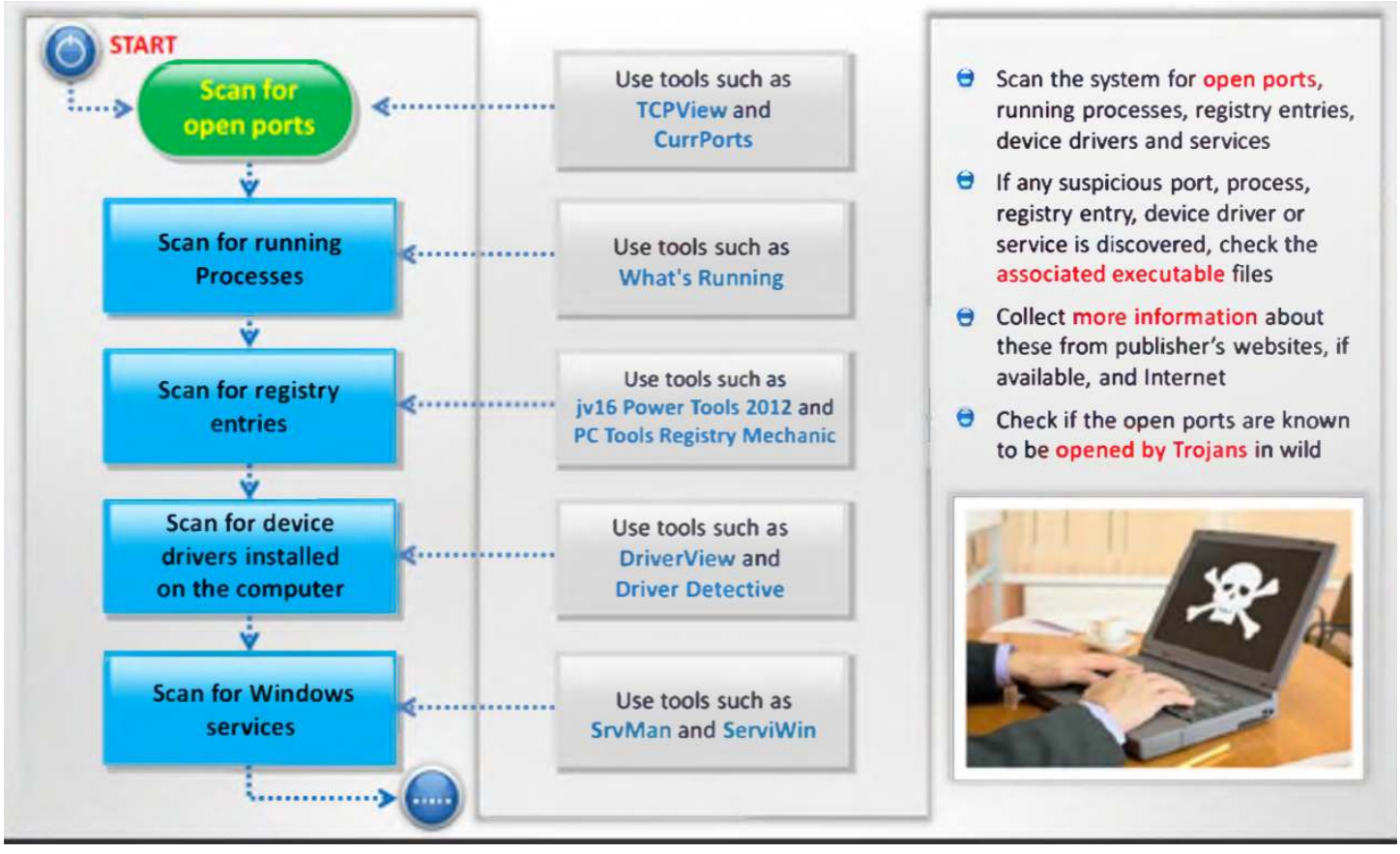
Port Redirection

- Communications are redirected to ports other than their original destination.
- Done by setting up a piece of software to listen on specified ports.
- When packets are received, the traffic is sent on to another system.

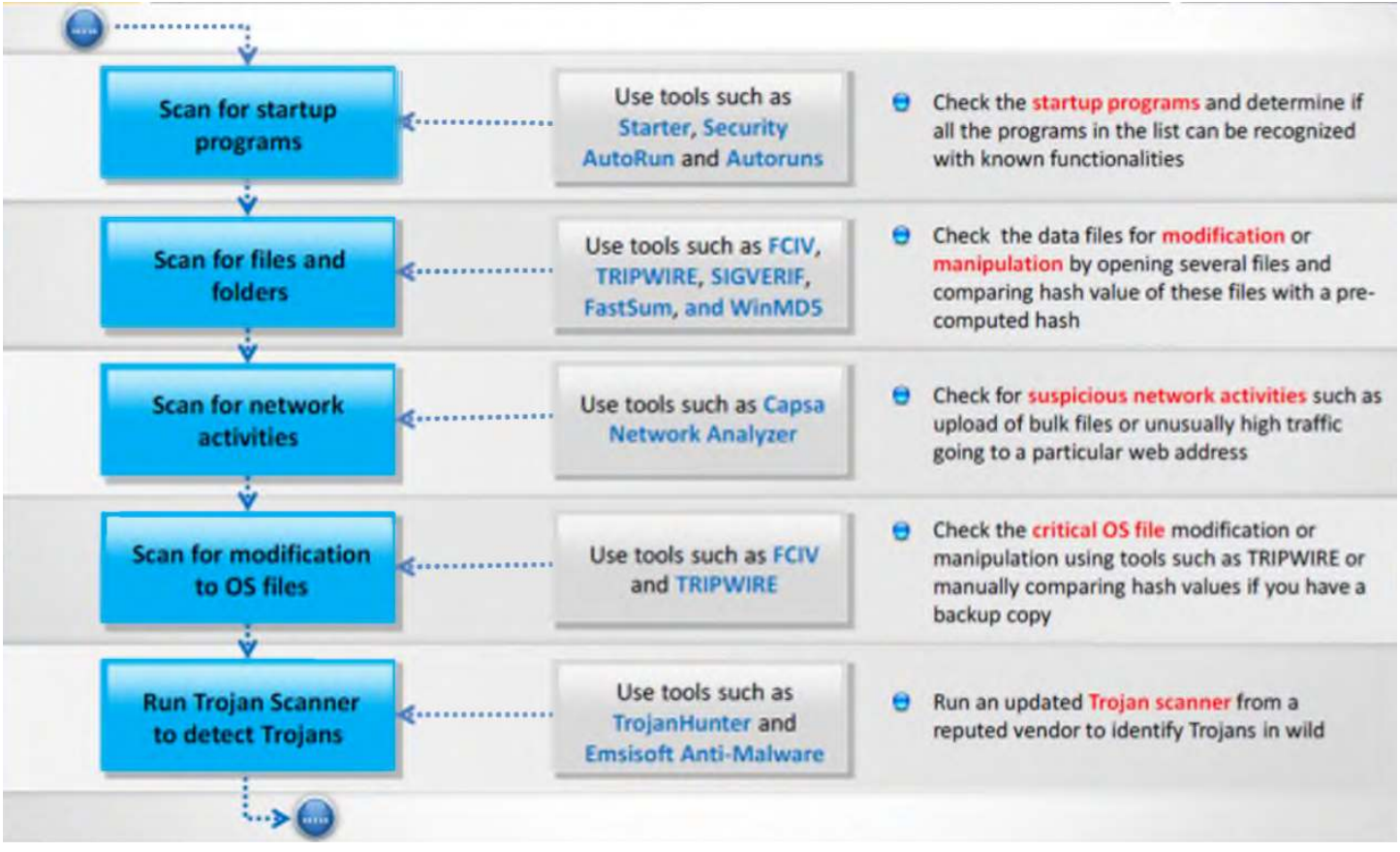
Port Redirection (Cont.)

- Netcat
  - A simple command-line utility available for Linux, UNIX, and Windows
  - Designed to function by reading information from connections using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) and doing simple port redirection on them as configured.

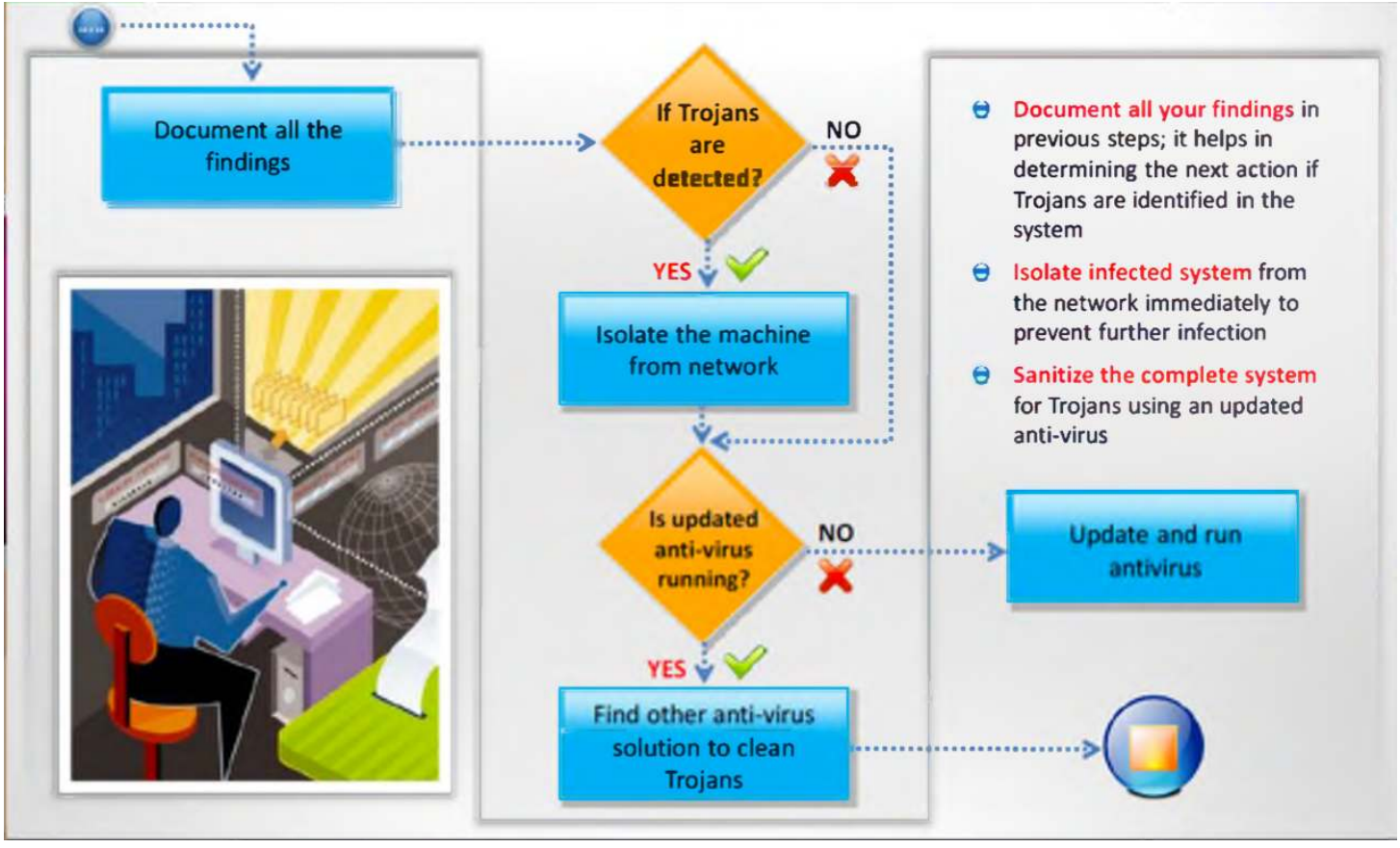
Pen Testing for Trojans and Backdoors



Pen Testing for Trojans and Backdoors (Cont'd)



Pen Testing for Trojans and Backdoors (Cont'd)



Summary

- Types of malware
- Malware removal and mitigation
- Trojan behavior, detection, and creation
- Backdoors and covert channels
- Ransomware