

Master of Cybersecurity Network scanning

Prepared by Dr. Nermin Hamza

Lecture 4

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل للتحفة وبناء المجتمعات

CYB740

Penetration test and Ethical hacking

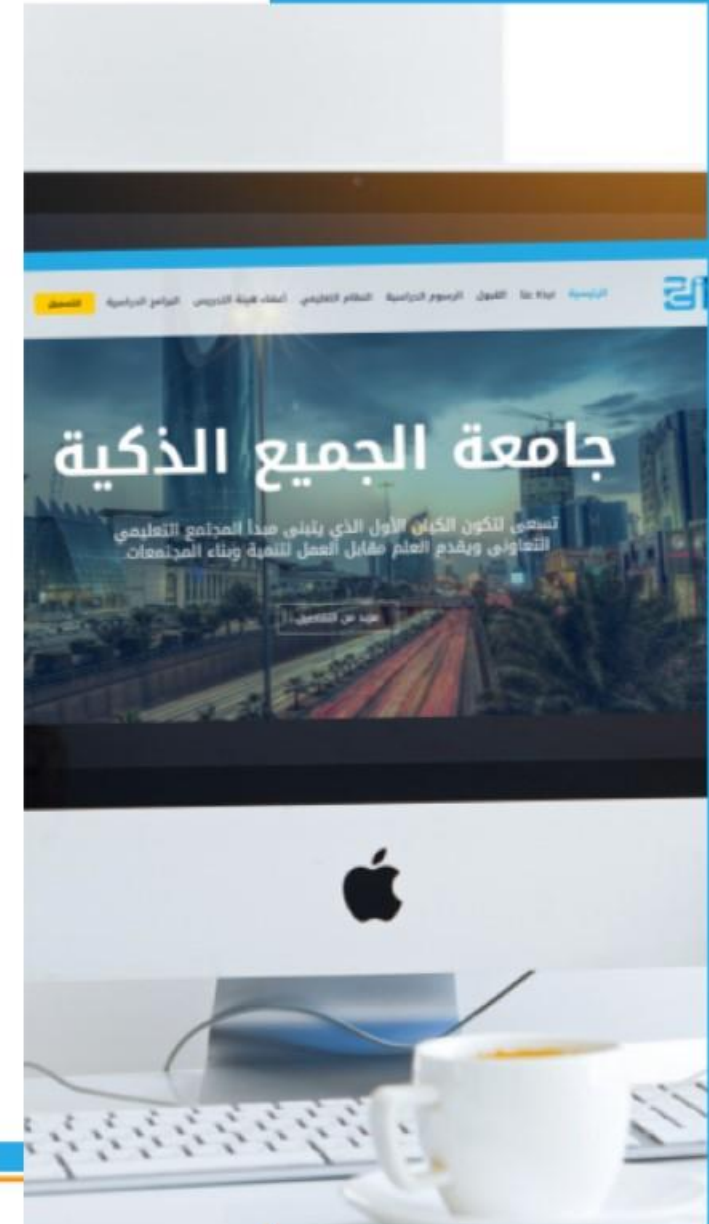


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Chapter 04

Outlines

- Introduction to Exploitation
- Different types of Exploits
- Exploits classification
- How Do Exploitation Occur?
- Malware
 - Trojans
 - Viruses
 - Ransomware



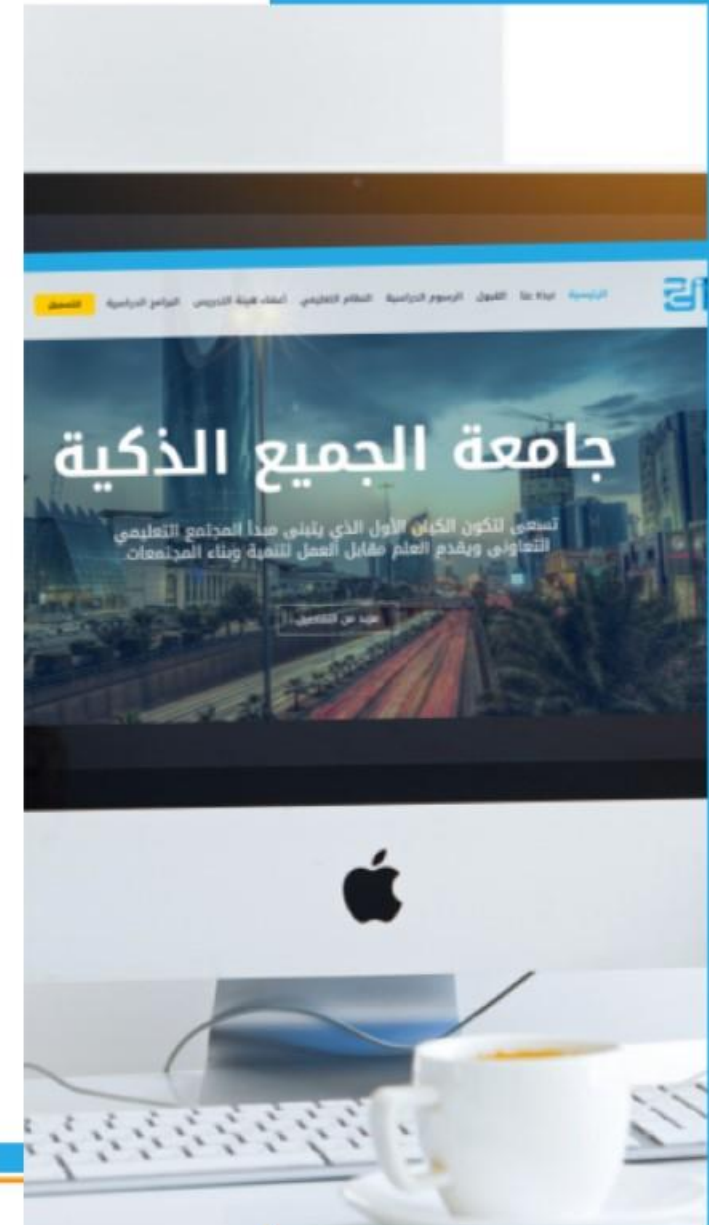
Chapter 04

Exploitation

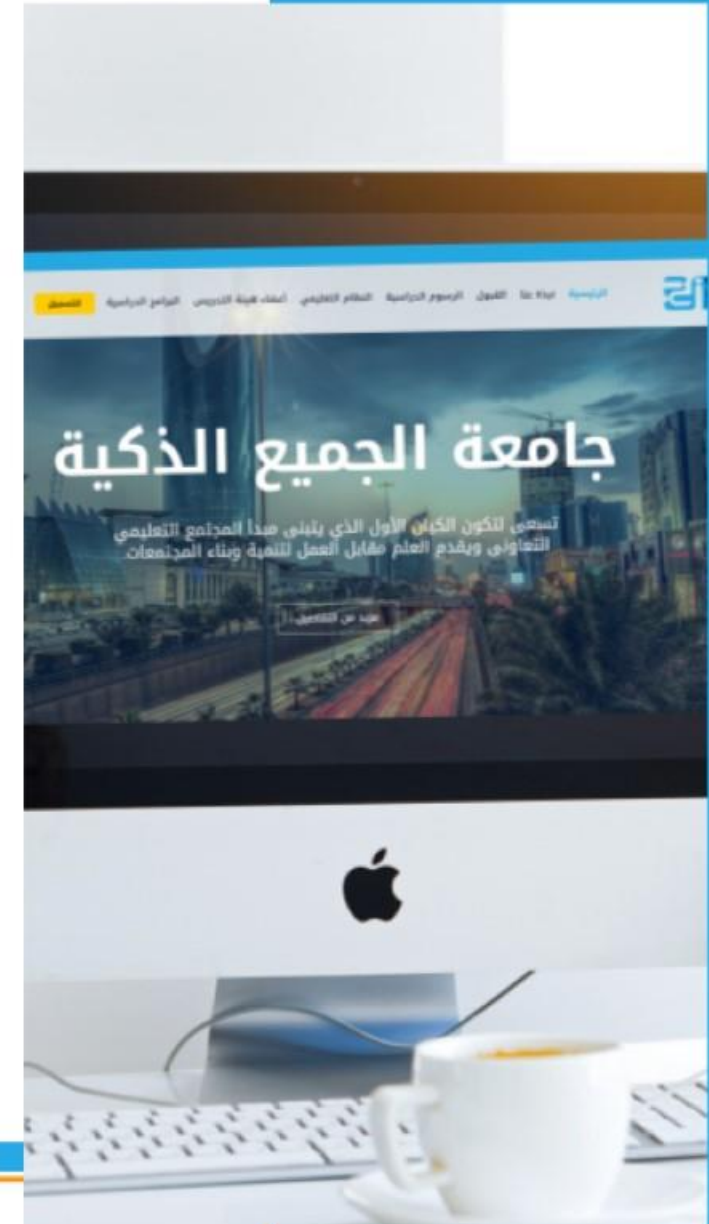
- Exploitation is the process of gaining control over a system



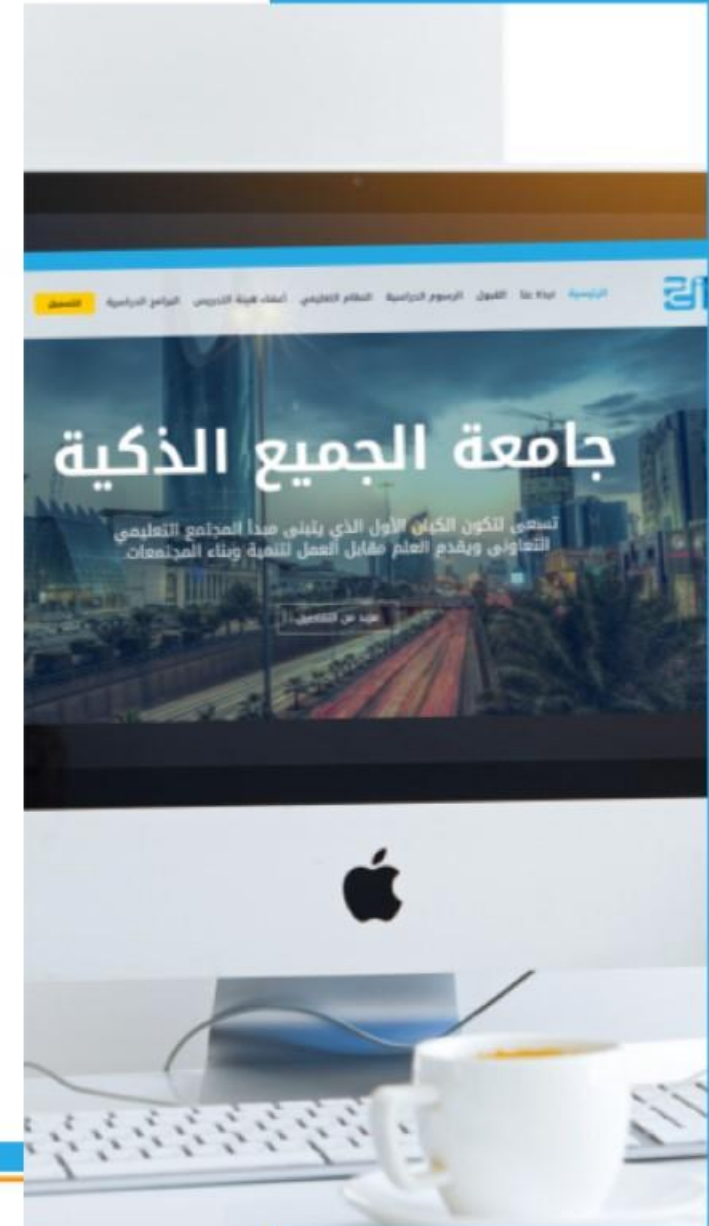
- It is important to understand that not every exploit leads to total system compromise.
- In many ways, **exploitation is an attempt to turn the target machine into a puppet** دمية that will execute your commands.



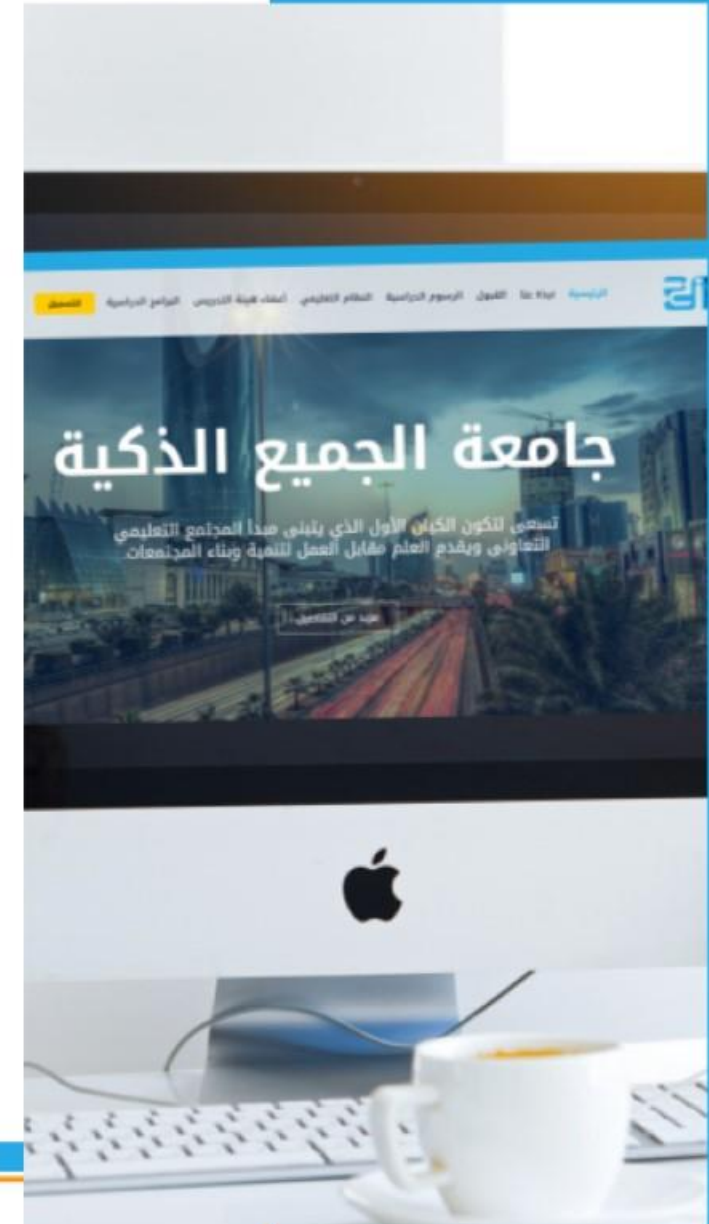
- Just to be clear, exploitation is the process of launching an exploit.
- Exploits are issues or bugs in the software code that give a hacker or attacker the ability to launch or execute a payload against the target system



- After gathering enough information about the target, the next and third phase of ethical hacking and penetration test is to gain access to the target by exploiting the vulnerabilities and weak points in targets identified during reconnaissance and scanning.

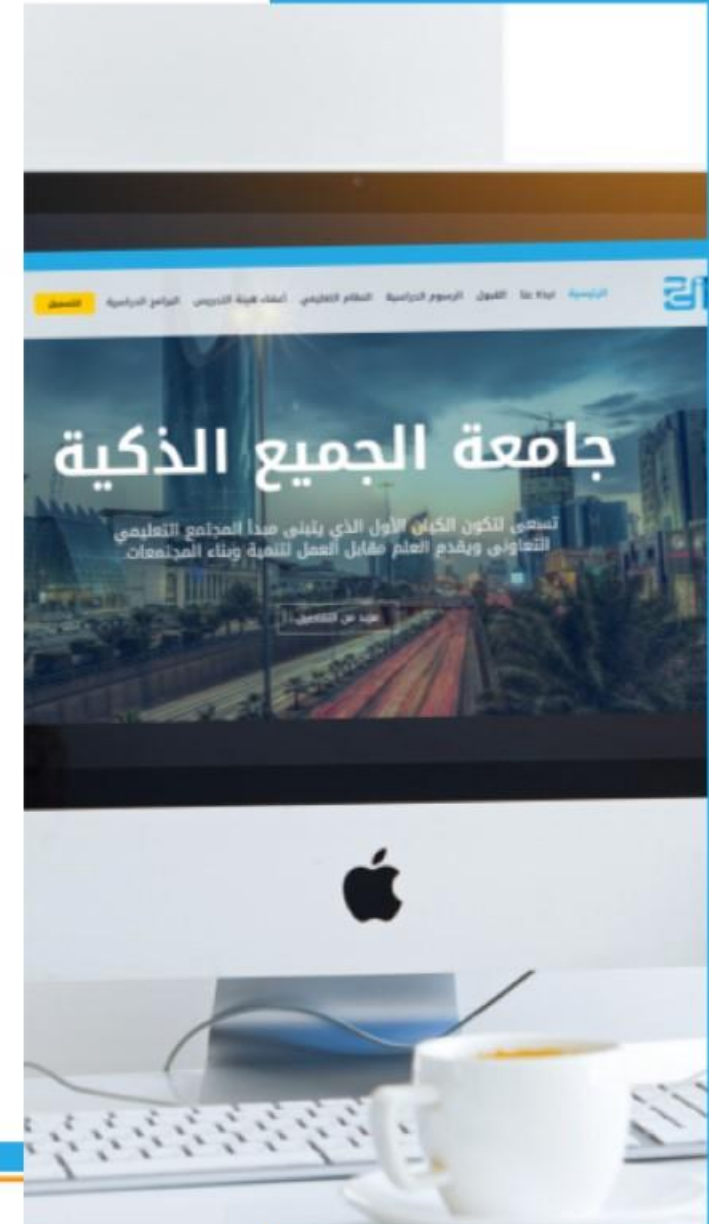


- A successful vulnerability **exploit** grants the control of the target to **penetration** testers.
- For example, an ethical hacker that identifies open FTP ports on the target during the scanning phase may be able to exploit the FTP service to plant malware.



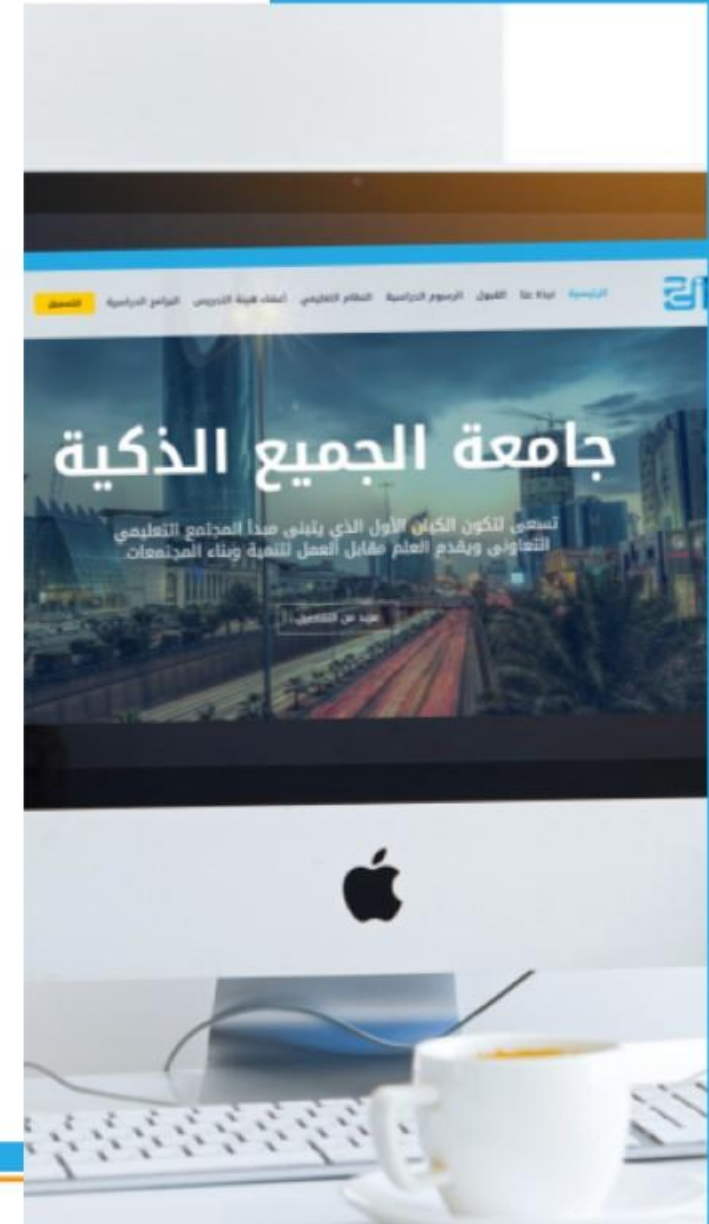
Different types of Exploits :

- **Known vulnerabilities:** Exploits security researchers know about and have documented. Exploits that target known vulnerabilities are often already patched but still remain a viable threat because of slow patching.
- **Zero-day exploits:** Vulnerabilities that have not been reported to the public or listed . This means cybercriminals have found the exploit before developers have been able to issue a patch, in some cases the developer may not even know of the vulnerability.



Exploits can be classified into five broad categories:

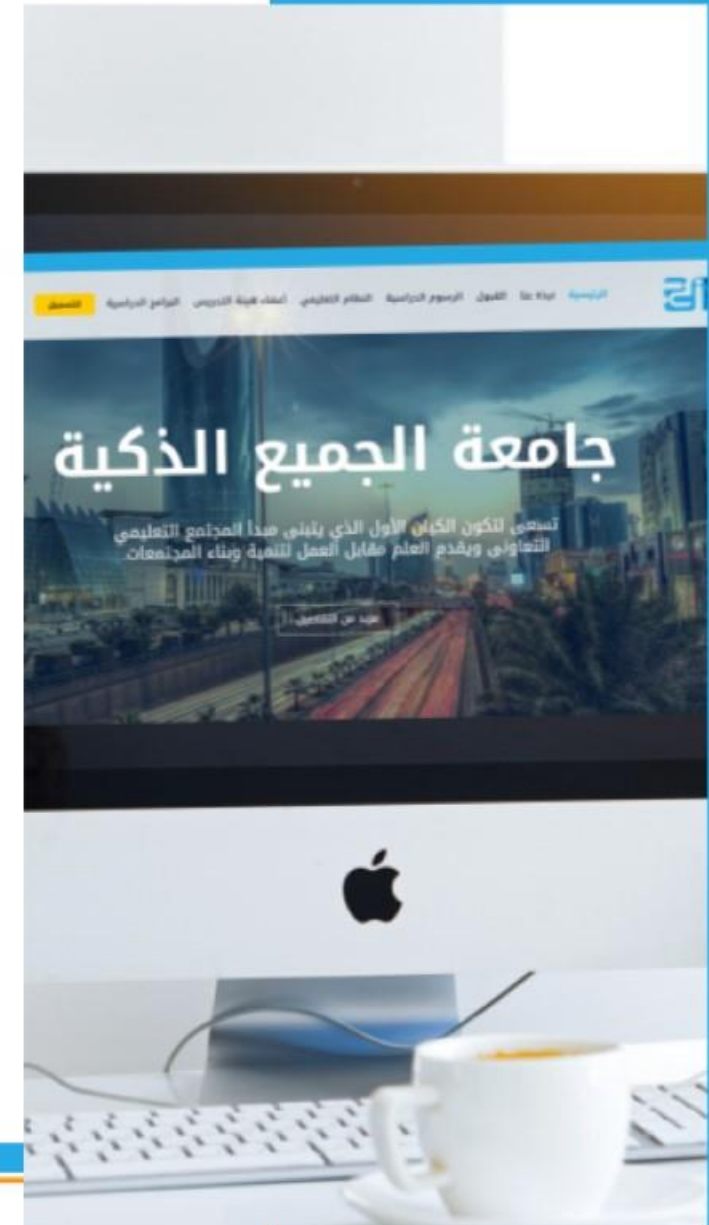
- **Hardware:** Poor encryption, lack of configuration management or firmware vulnerability.
- **Software:** Memory safety violations (buffer overflows, over-reads, dangling pointers), input validation errors (code injection, cross-site scripting (XSS), directory traversal, email injection, format string attacks, HTTP header injection, HTTP response splitting, SQL injection).
- **Network:** Unencrypted communication lines, man-in-the-middle attacks, domain hijacking, poor network security, lack of authentication or default passwords.
- **Personnel:** Poor setting policy and process, lack of security awareness training,, poor password management or falling for common social engineering attacks like phishing.
- **Physical site:** Poor physical security and lack of keycard access control.



How Do Exploits Occur?

There are several ways exploits occur:

- **Remote exploits:** Works over a network and exploits the vulnerability without prior access to the vulnerable system.
- **Local exploits:** Requires prior access to the vulnerable system and increases the privilege of the attacker past those granted by the security administrator.
- **Client exploits:** Exploits against client applications exist and usually consist of modified servers that send an exploit when accessed with a client application.

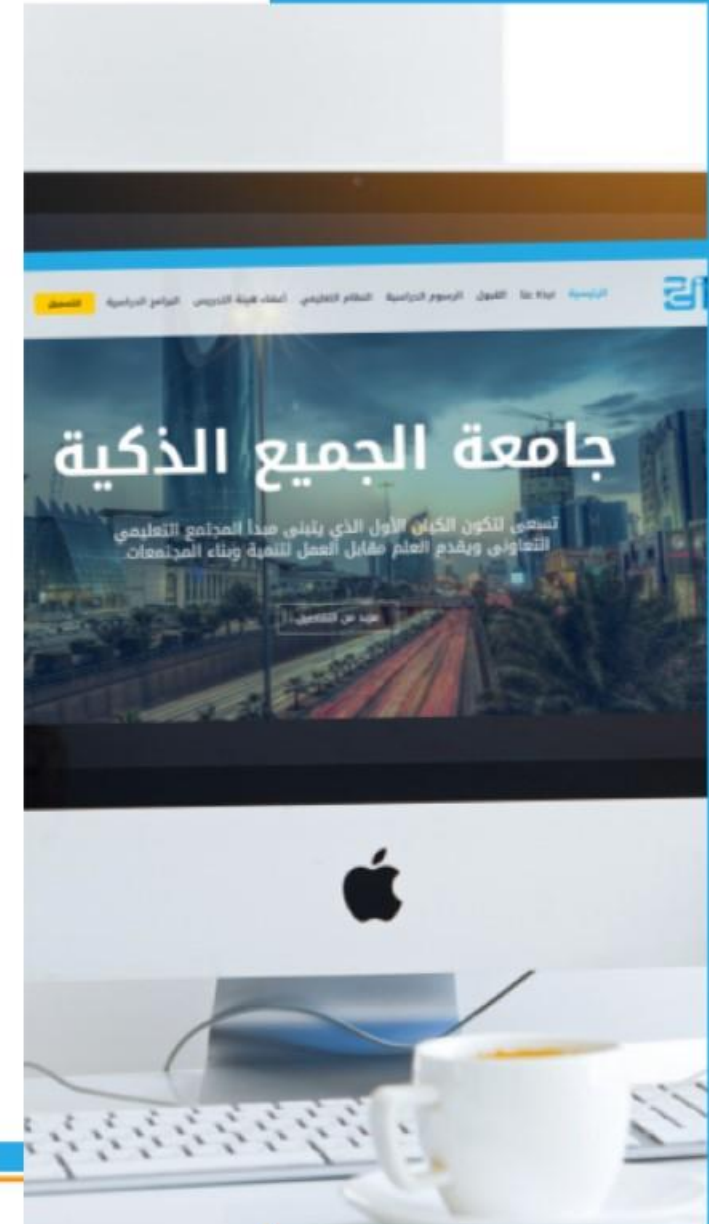


Chapter 04

Exploitation

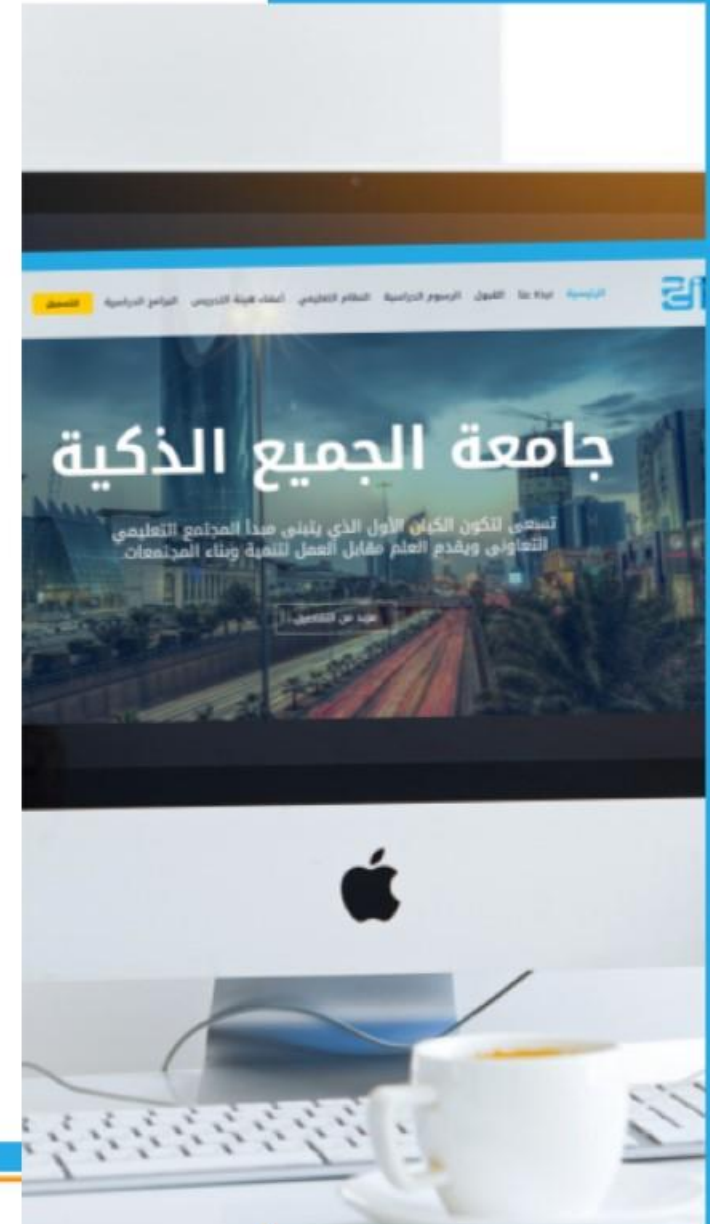
Hackers typically use many hacking tools and techniques to simulate attempted unauthorized access, including:

- Malware
- Password crack
- Remote exploitation
- Client exploitation
- Sniffing and Phishing
- Injection attacks
- Web hacking

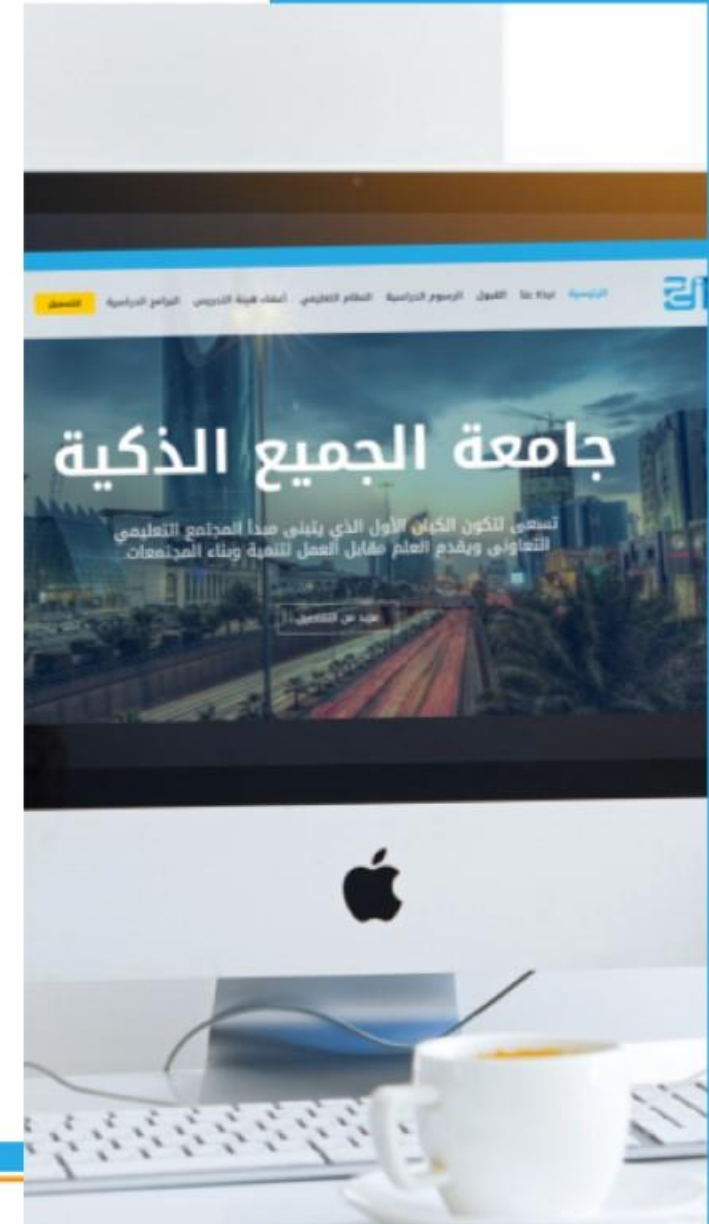


Chapter 04

Malware



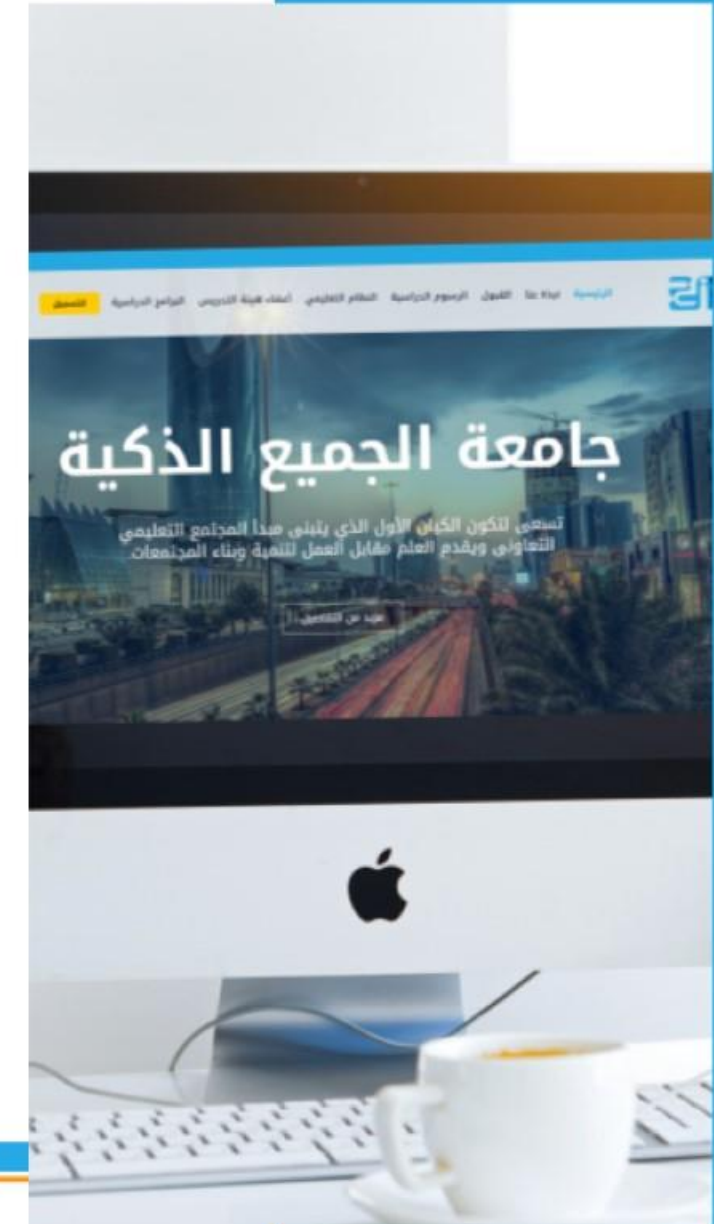
- Malware is malicious software that damages or disables computer systems and gives limited or full control of the system to the malware creator .



Chapter 04

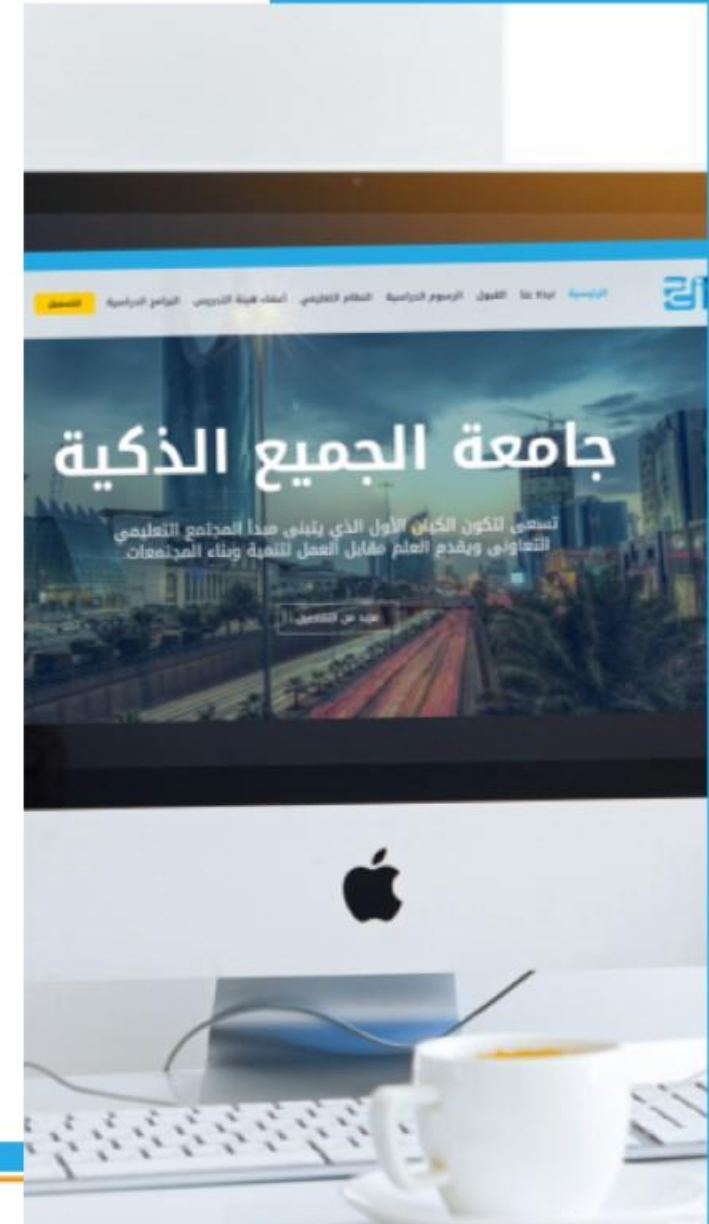
Malware

Type	What It Does	Real-World Example
Ransomware	disables victim's access to data until ransom is paid	RYUK
Fileless Malware	makes changes to files that are native to the OS	Astaroth
Spyware	collects user activity data without their knowledge	DarkHotel
Adware	serves unwanted advertisements	Fireball
Trojans	disguises itself as desirable code	Emotet
Worms	spreads through a network by replicating itself	Stuxnet
Rootkits	gives hackers remote control of a victim's device	Zacinlo
Keyloggers	monitors users' keystrokes	Olympic Vision
Bots	launches a broad flood of attacks	Echobot
Mobile Malware	infects mobile devices	Triada
Wiper Malware	A wiper is a type of malware with a single purpose: to erase user data beyond recoverability.	WhisperGate



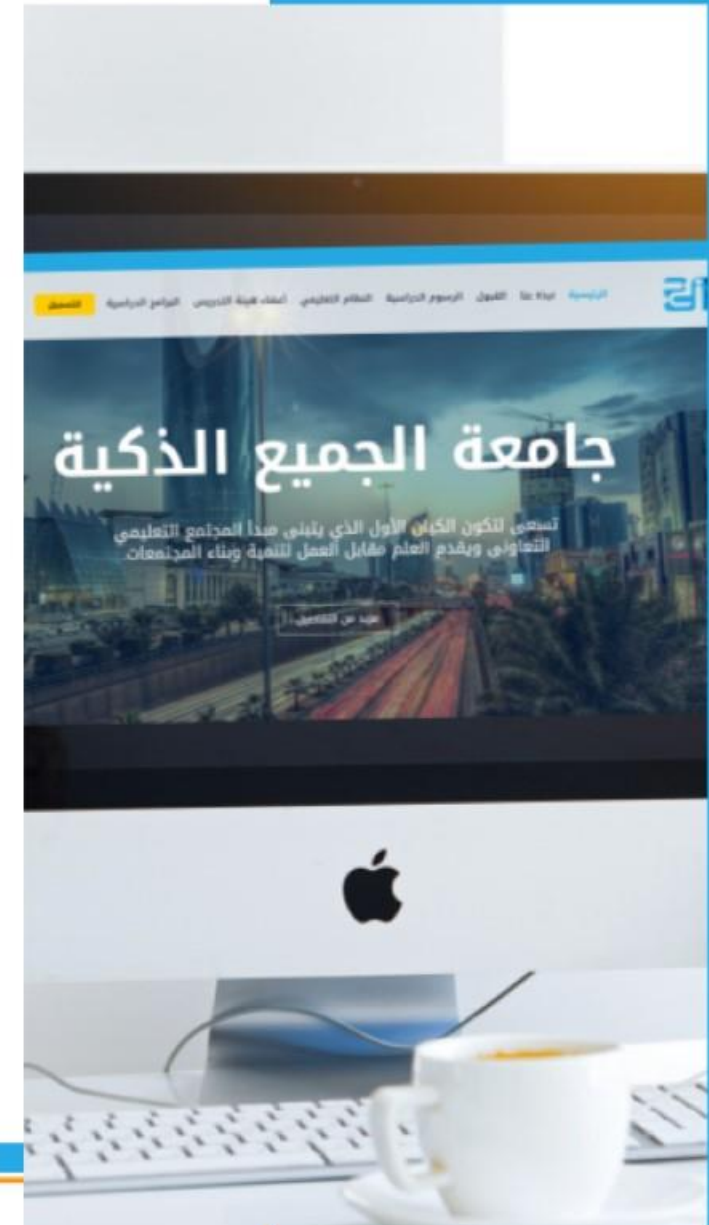
How can Malware get into a system

- Removable devices
- Attachments
- Browser and email software bugs
- Legitimate “shrink-wrapped” software packaged by a disgruntled employee
- Instant Message applications
- Downloading files , games from the internet



Chapter 04

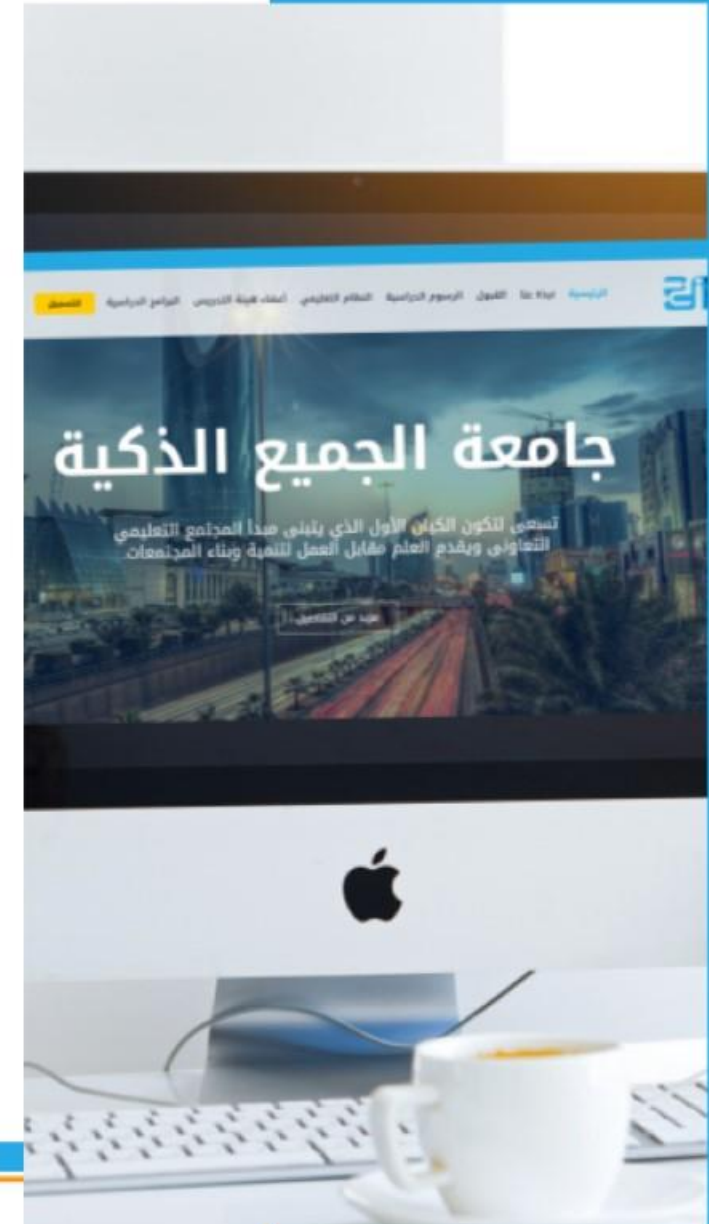
Trojan



Chapter 04

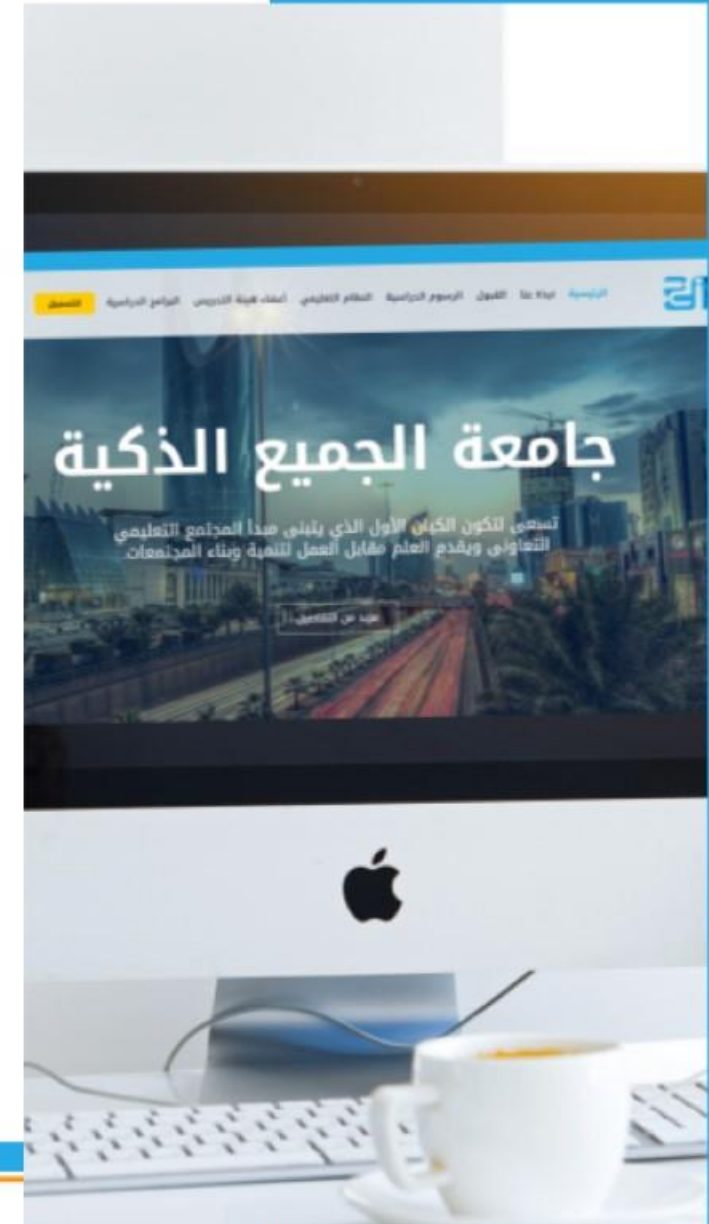
Trojan

- Hiding payload inside of some legitimate program that would run normally, with the payload running in the background.



How Much Damage Can Trojans Do?

- So, still thinking that the attachment was legitimate, you unwittingly downloaded and installed a Trojan.
- What happens now? The malware executes and starts damaging your computer, but the amount of damage depends on how the hacker designed the Trojan.
- In general, Trojan malware can:
 - Delete your files
 - Install additional malware
 - Modify data on your device
 - Copy your data
 - Disrupt your device's performance
 - Steal your personal information

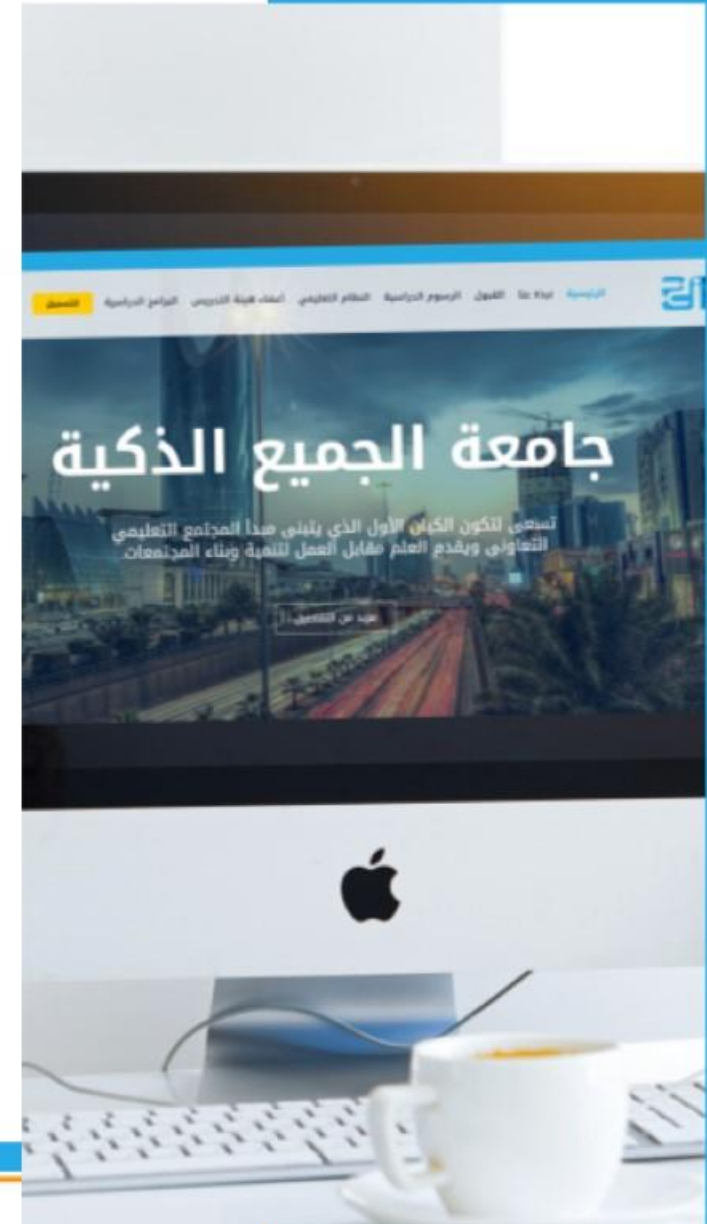


Chapter 04

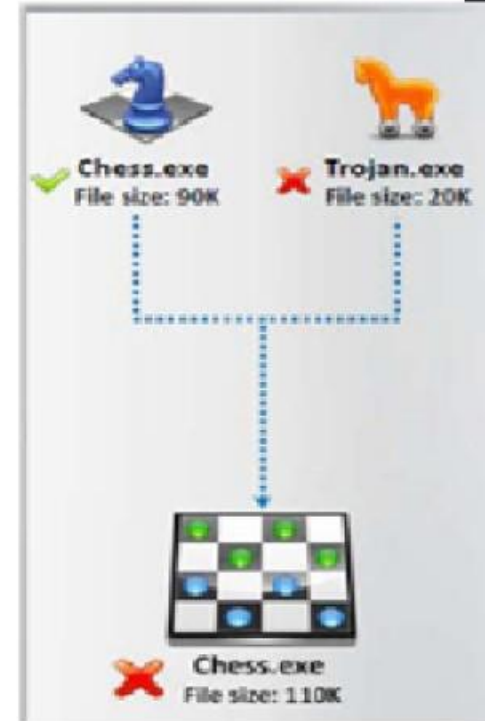
Trojan

How to infect systems by Trojan

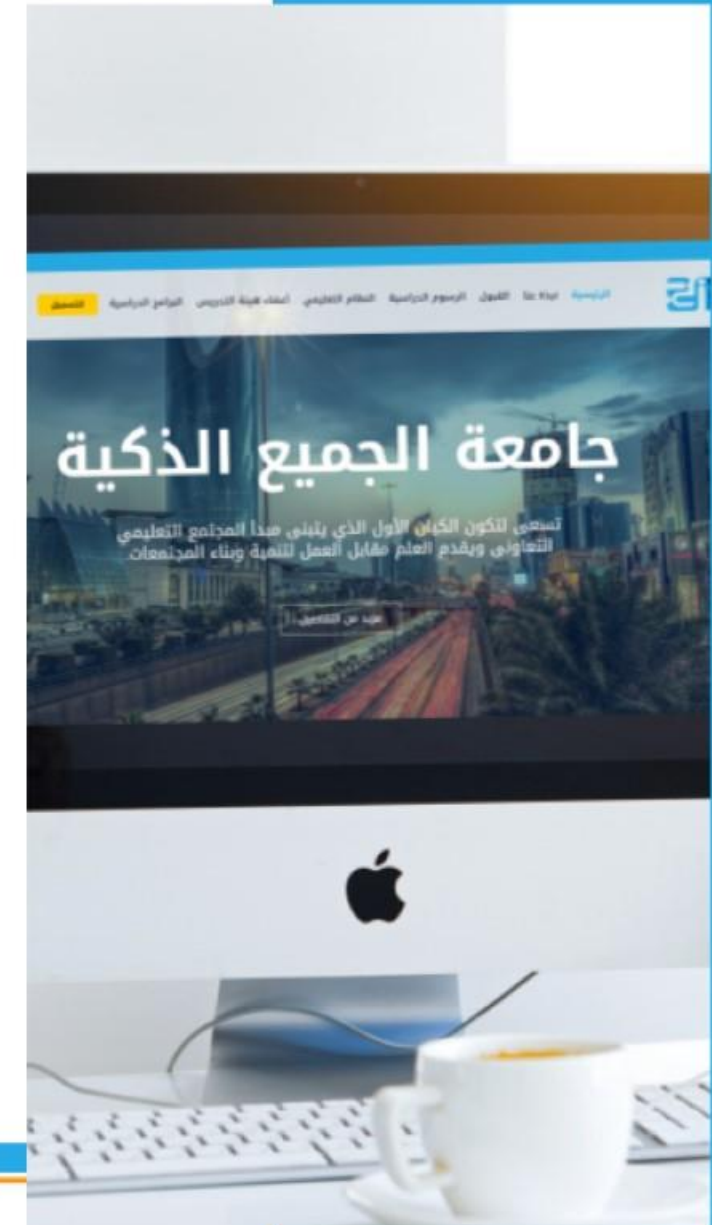
- Prepare Trojan
- Create Wrapper (using Wrapper Tool)
- Execute Damage



- 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.



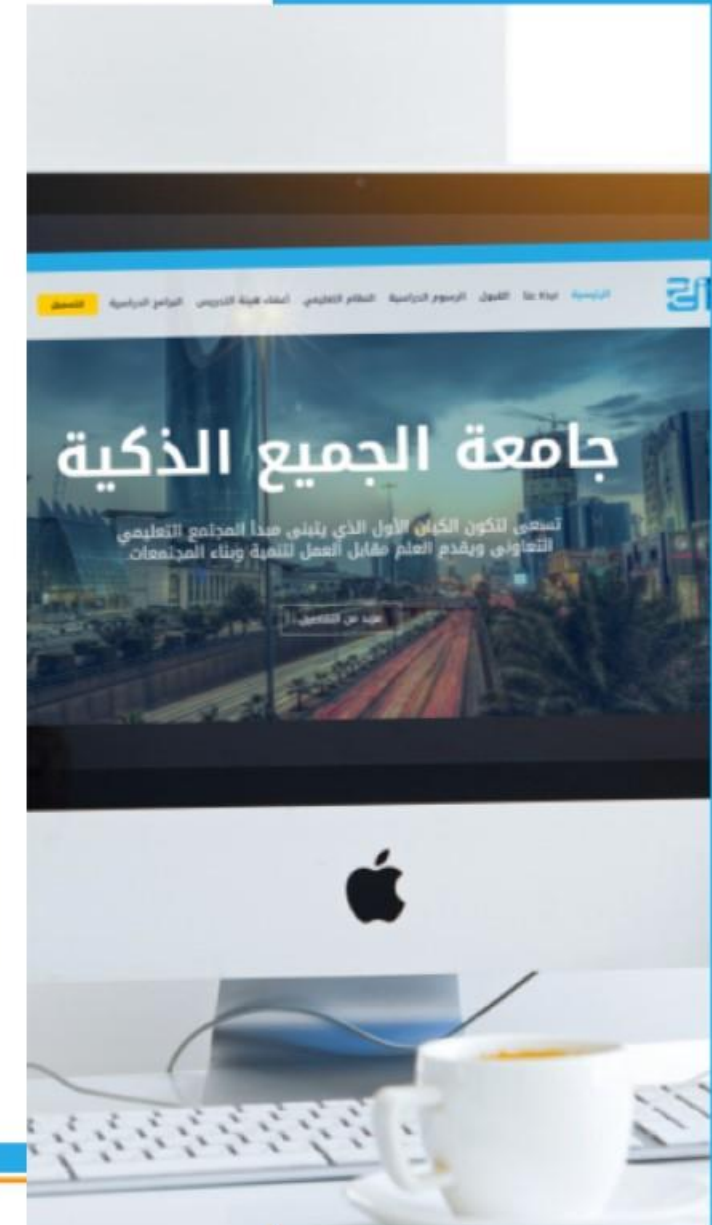
- Proxy Trojan : is usually a standalone application that allows remote attackers to use the victim's computer as proxy to connect to the internet.
- Proxy server Trojan when infected starts a hidden proxy server on the victim's computer
- Many machines on the internet are infected with proxy server using this techniques.



Chapter 04

Trojans: FTP Trojans

- FTP Trojans install an FTP server on the victim's machine which open FTP ports
- An attacker can then connect to the victim's machine
- Using FTP port to download any files that exist on the victim's computer

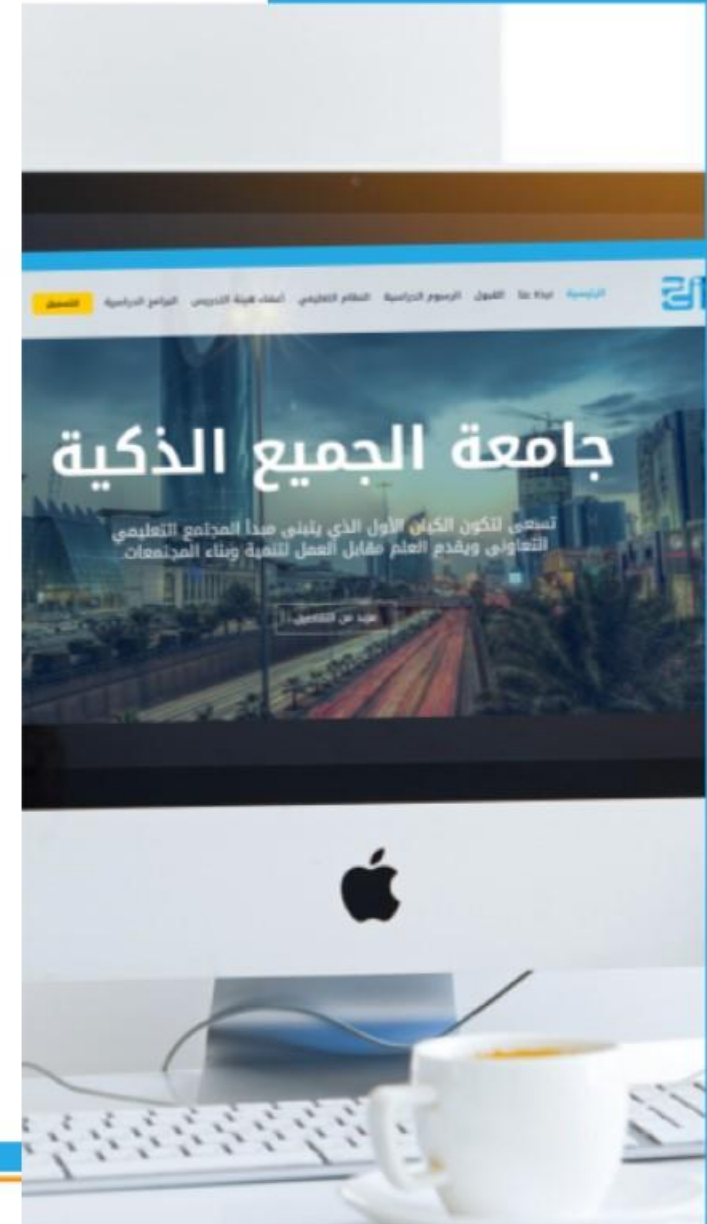


- How to use nc command to give control to another machine
- Trojan server is installed on the victim's machine , which opens a ports for attacker to connect
- The client is installed on the attacker's machine , which is used to launch a command shell on the victim's machine.



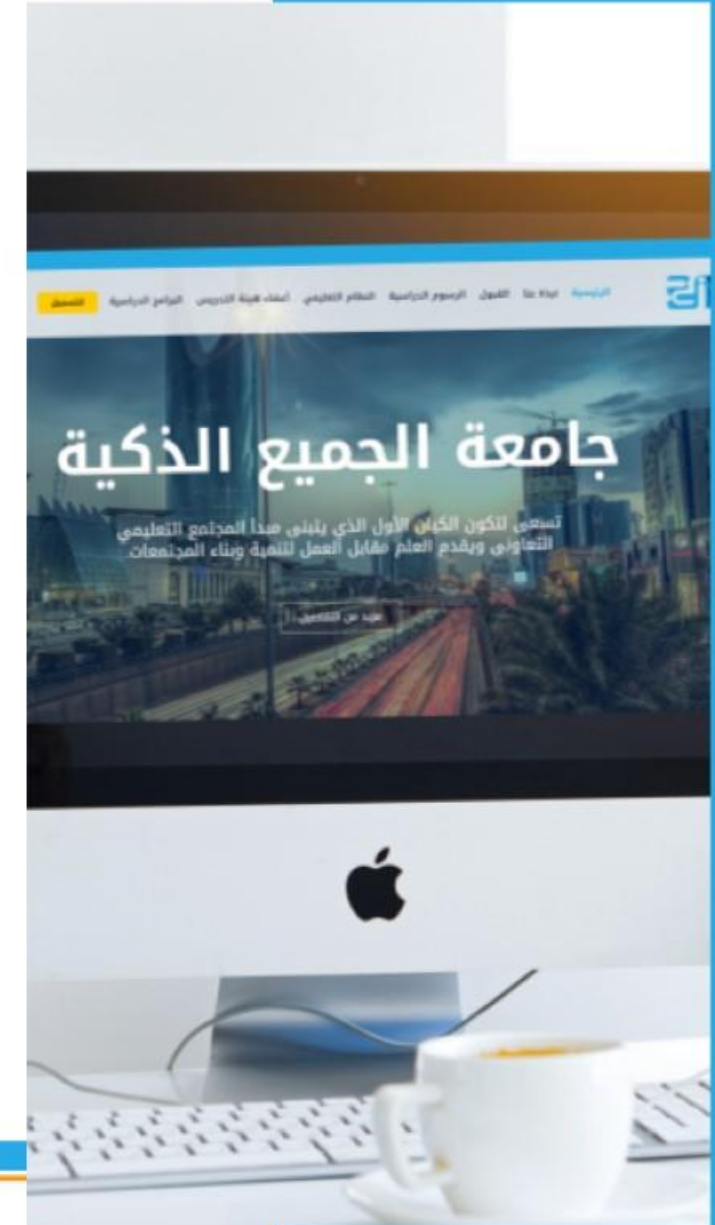
Note that :

- Trojans spread more slowly than other malware because they don't self-replicate.

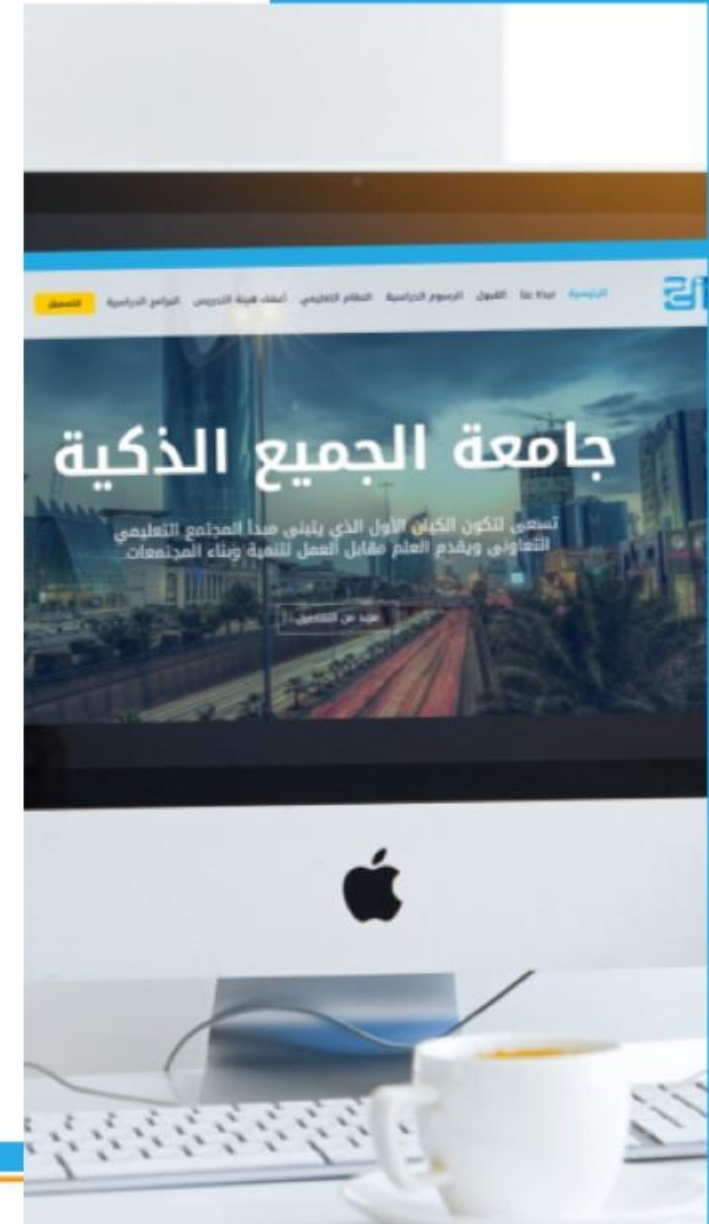


- **SubSeven:**

- The SubSeven Trojan is a RAT, which gives hackers remote control over Windows computers and networks. When it infiltrates a computer, SubSeven modifies system files and registries, causing the Trojan to execute upon startup.

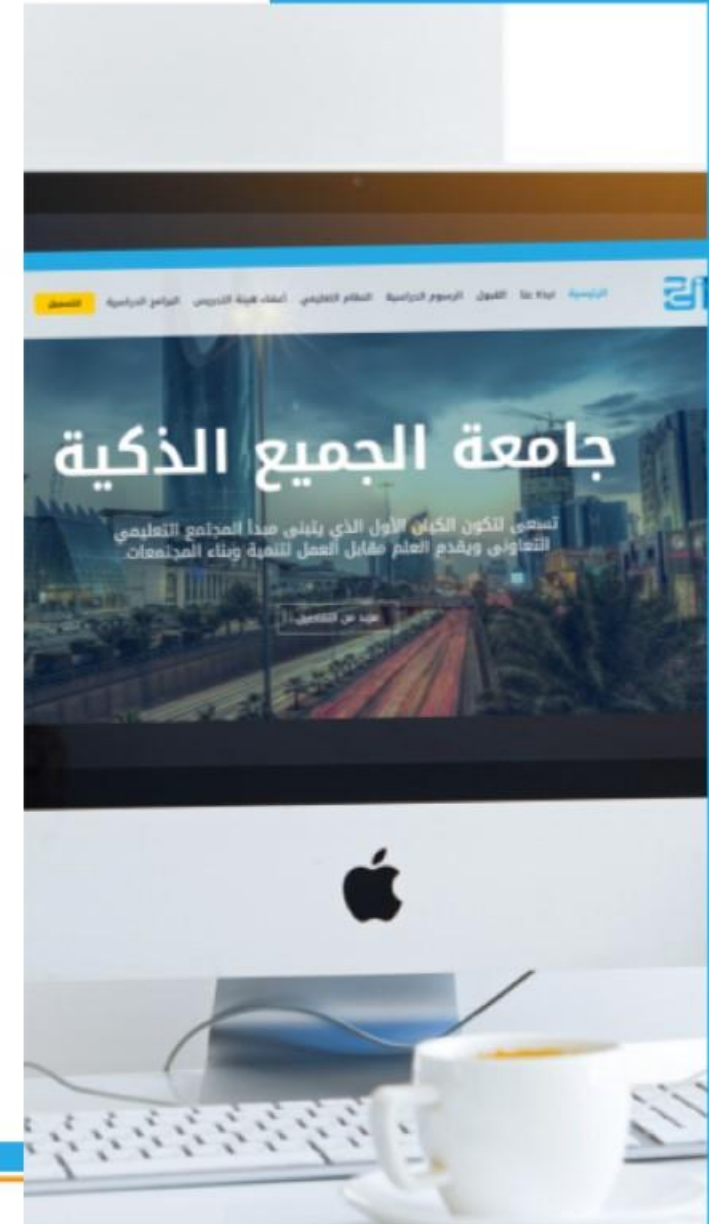


- **Zeus (Zbot):** Originally, the Zeus Trojan stole financial information from its targets by logging keystrokes to steal passwords.
- Instead of performing the attacks himself, the maker of Zeus sold its source code to cybercriminals, which is partly why Zeus became widespread. However, since the developer's retirement in 2010, the source code became available publicly.
- That means that the development of new variants of Zeus continues to this day.



How to Remove a Trojan Virus

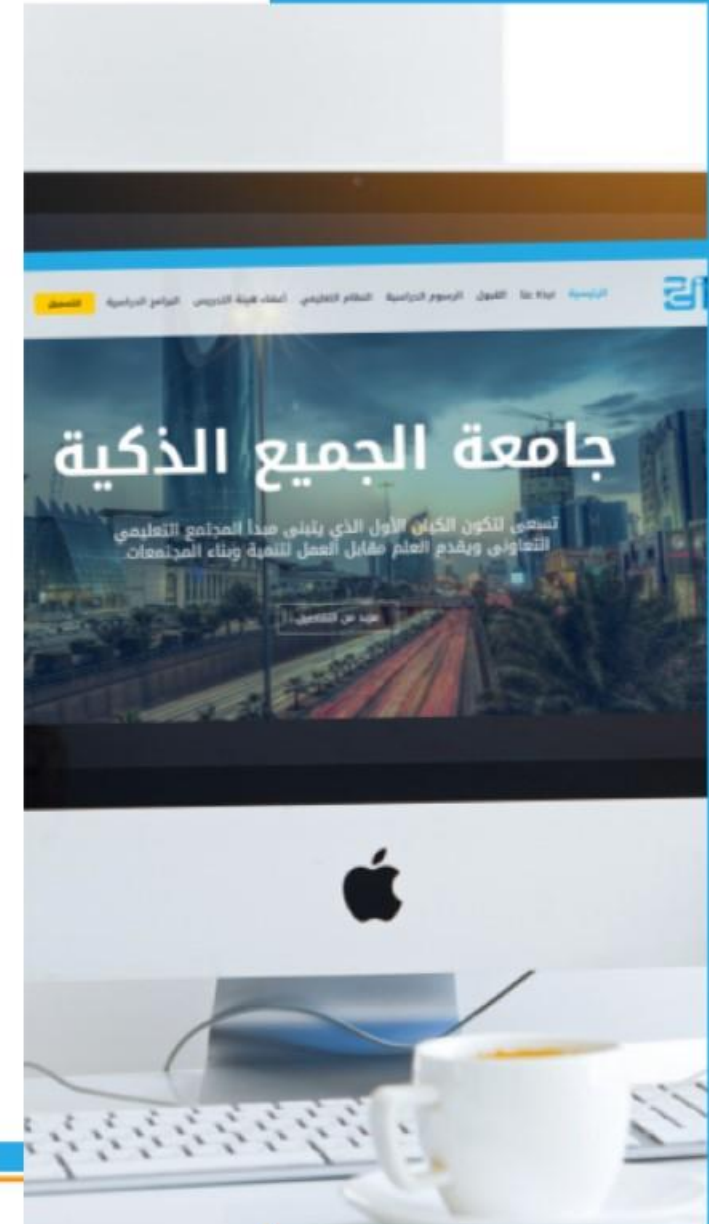
- Before you discover all the places a Trojan can invade your computer, let's first learn how to get rid of them.
- You can remove some Trojans by disabling startup items on your computer which don't come from trusted sources.
- For the best results, first reboot your device into safe mode so that the virus can't stop you from removing it.



Chapter 04

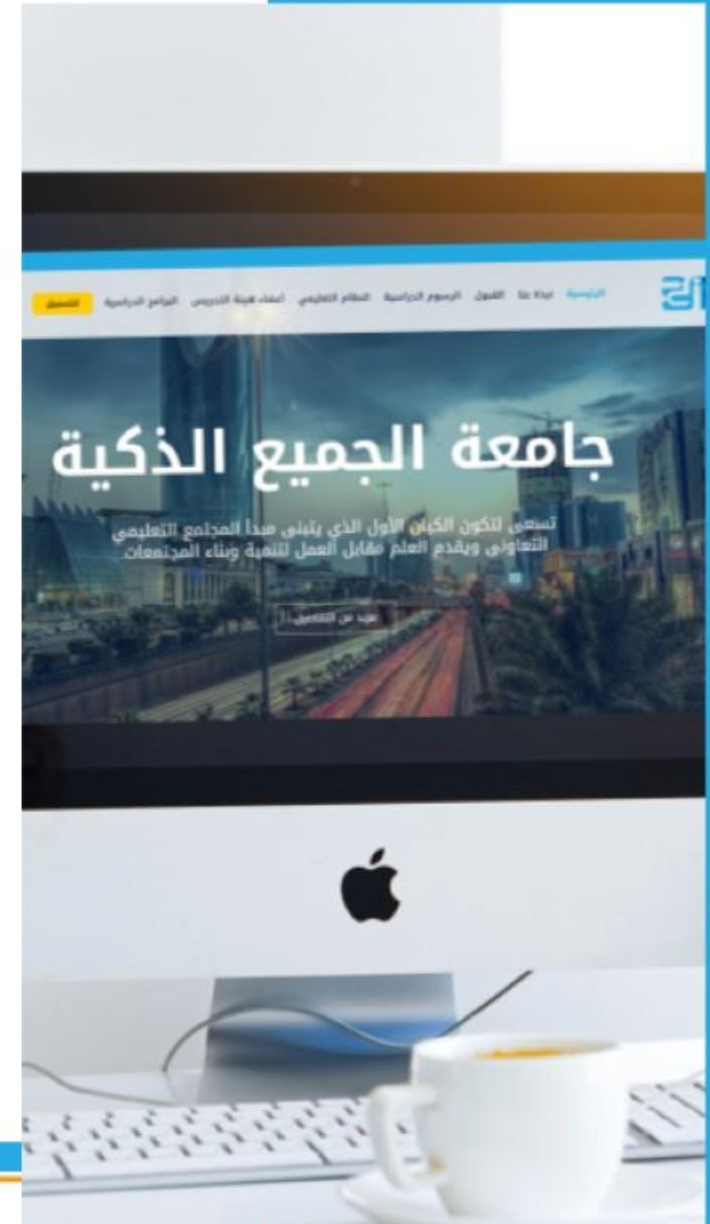
Trojans

- Please carefully ensure you know which specific programs you're removing because you could slow, disable or cripple your system if you remove basic programs your computer needs to function.
- Installing and using a trusted antivirus solution is also one of the top ways to get rid of trojans.
- An effective antivirus program searches for valid trust and app behavior, as well as trojan signatures in files in order to detect, isolate and then promptly remove them.



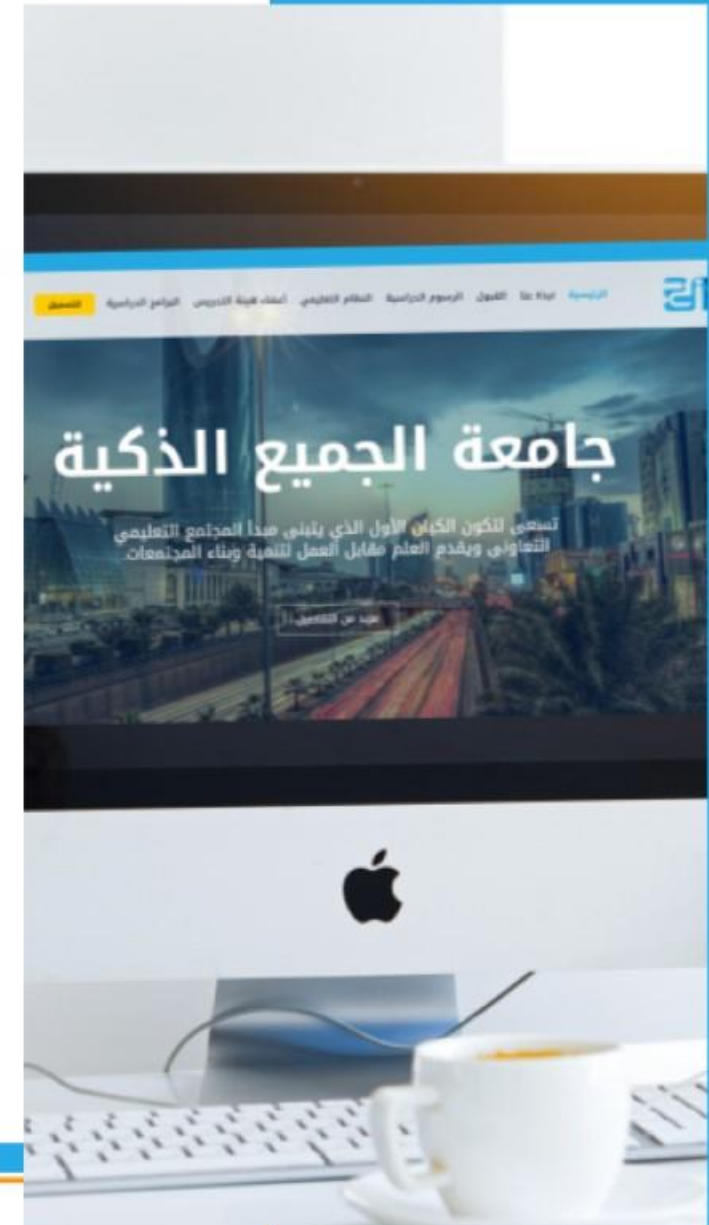
Chapter 04

Virus

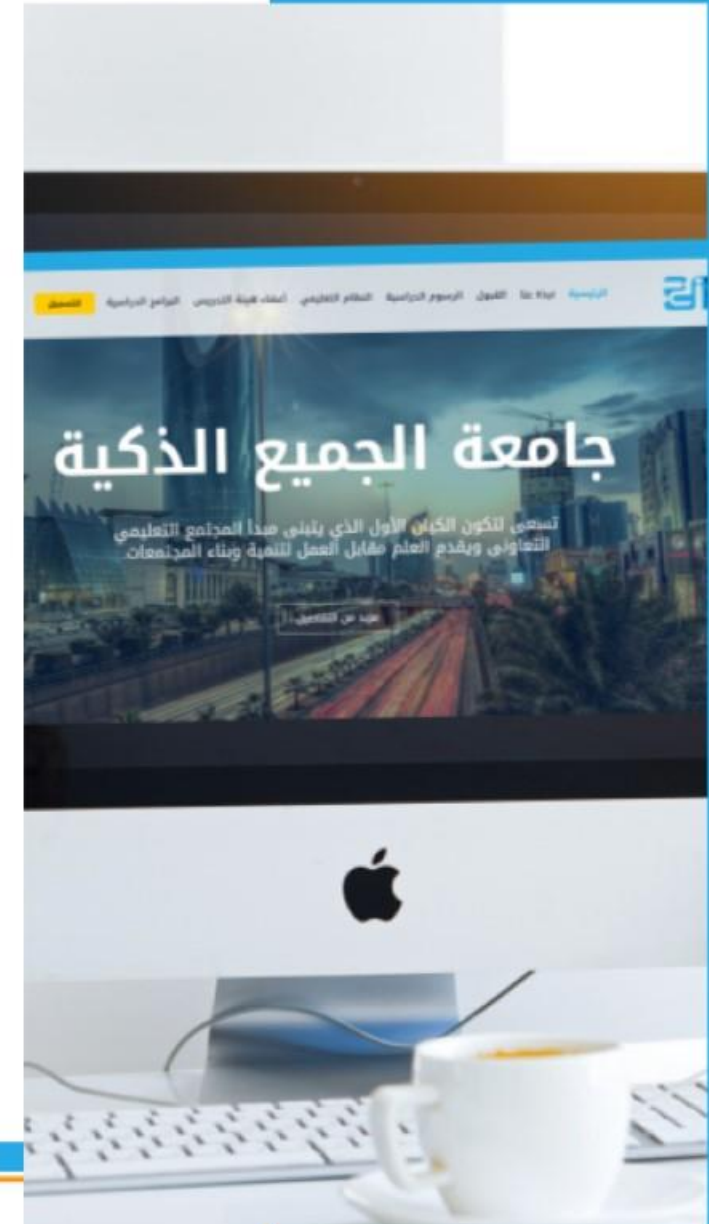


What is a virus?

- A Computer Virus is one of the malware.
- It is computer program that spreads or replicates by copying itself.
- The main parts of a virus' code are :-
 - The replication routine.
 - The payload routine.



- The typical life-cycle of a computer virus takes place in four stages;
 1. The dormant phase **خامل**
 2. Propagation phase **التكاثر**
 3. The triggering phase **المشغل**
 4. And the execution phase **التنفيذ**.

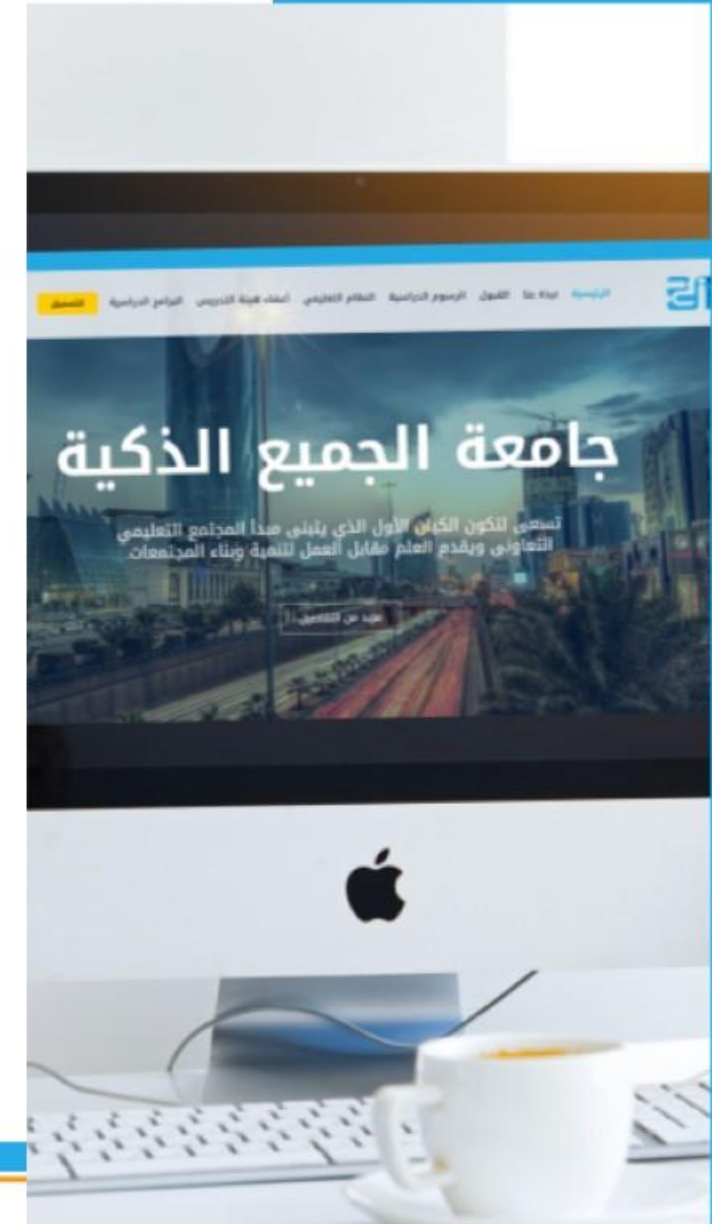


Dormant phase

- The virus is idle in the dormant phase. It has accessed the target device but does not take any action.

Propagation phase

- In the propagation phase, the virus starts propagating by replicating itself.
- The virus places a copy of itself into other programs or accomplishes certain system areas on the disk.
- Each infected program will contain a clone of the virus, which will enter its own propagation phase as well.

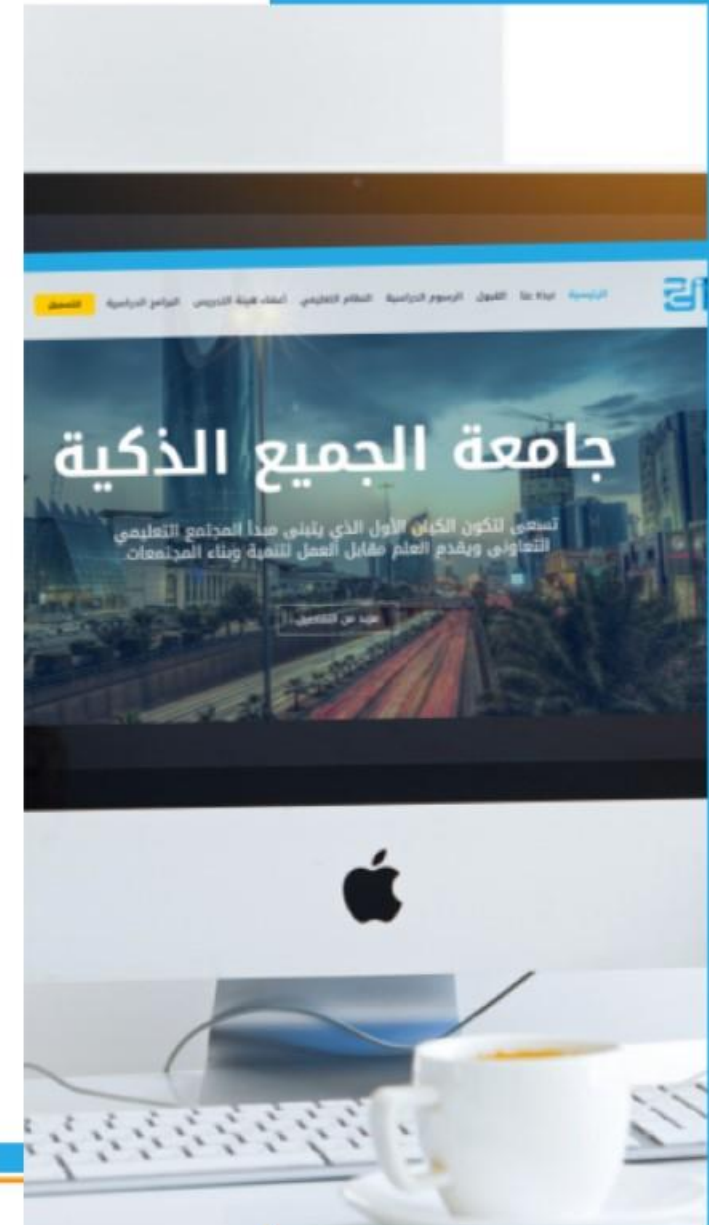


Triggering phase

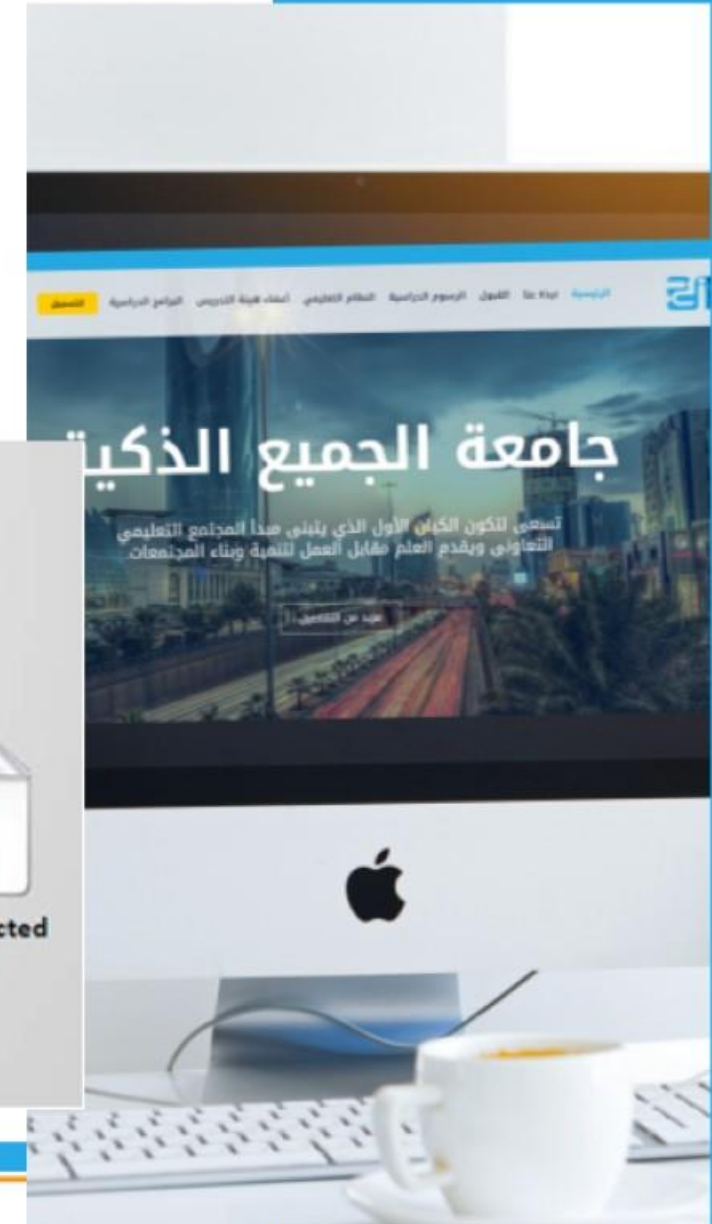
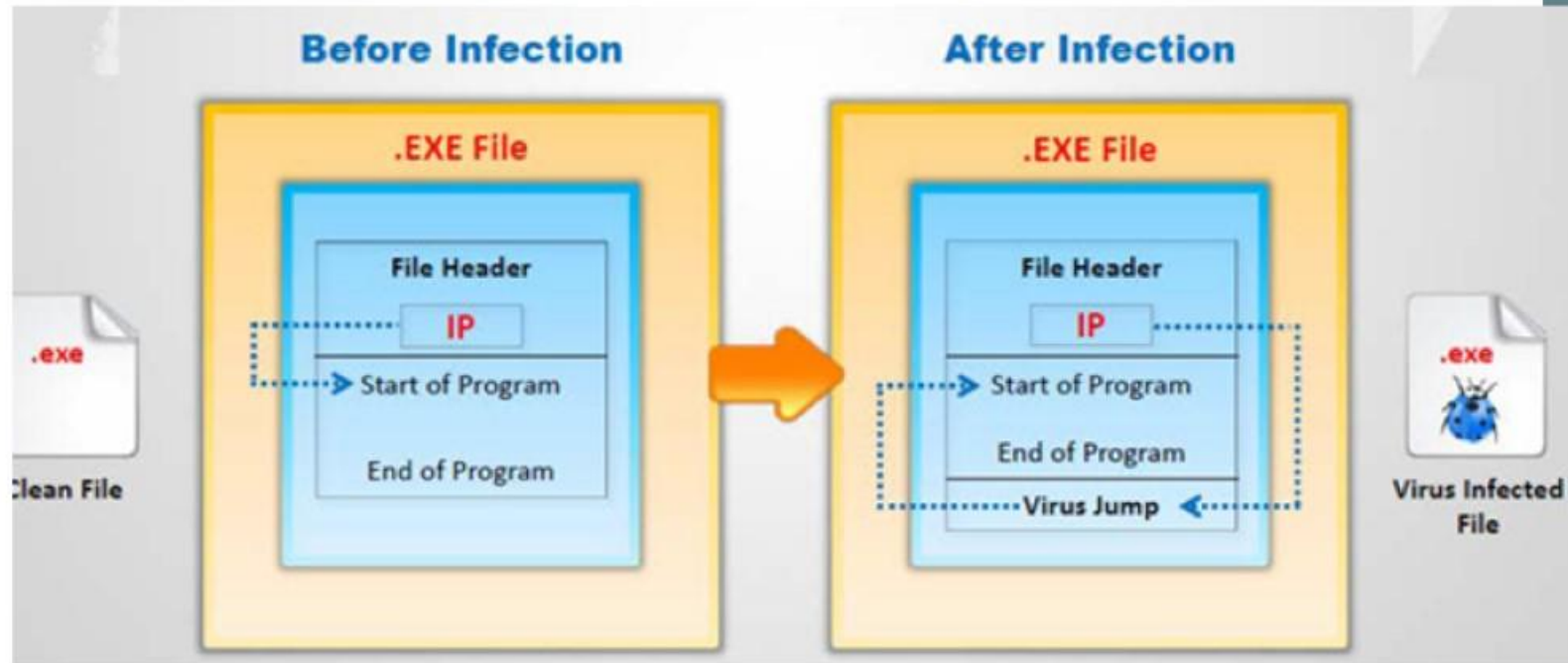
- The triggering phase starts when the dormant virus is activated. It will perform the actions it is supposed to accomplish. This phase can be caused by various system events like the count of the times the virus has cloned or after a set time interval has elapsed.

Execution phase

- In the execution phase, the payload will be released. It can harm deleting files, crashing the system, and so on. It can be harmless too and pop some humorous messages on screen.

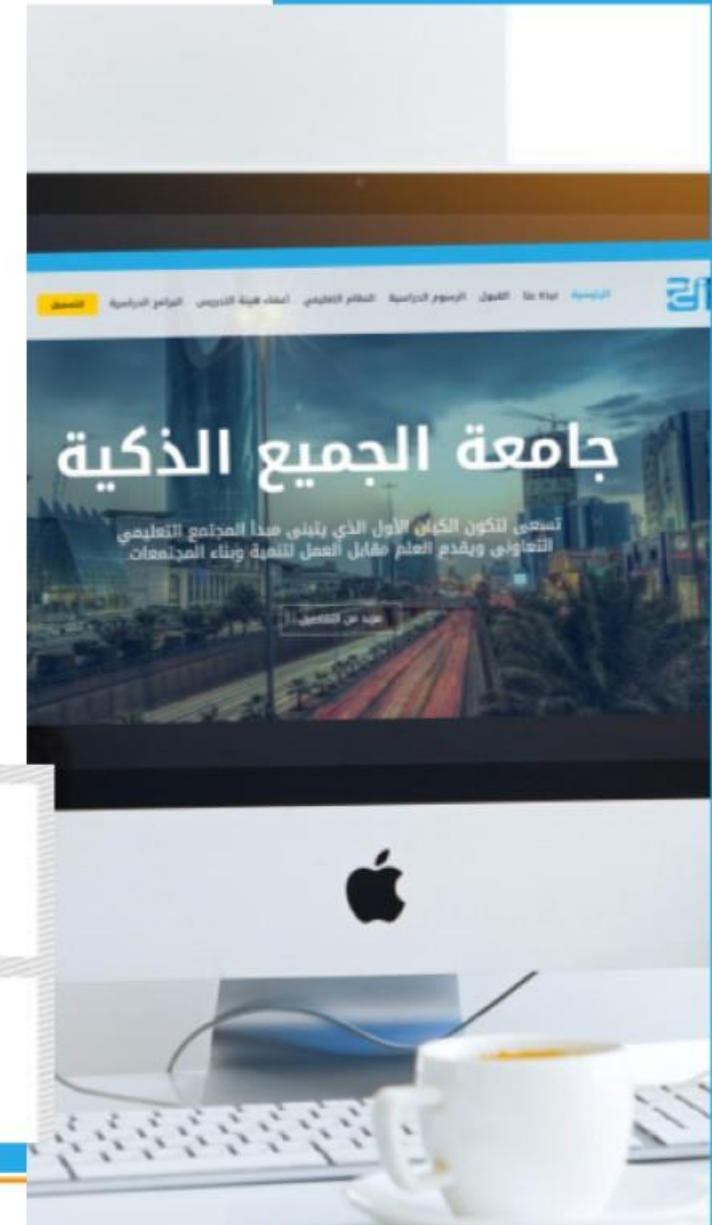
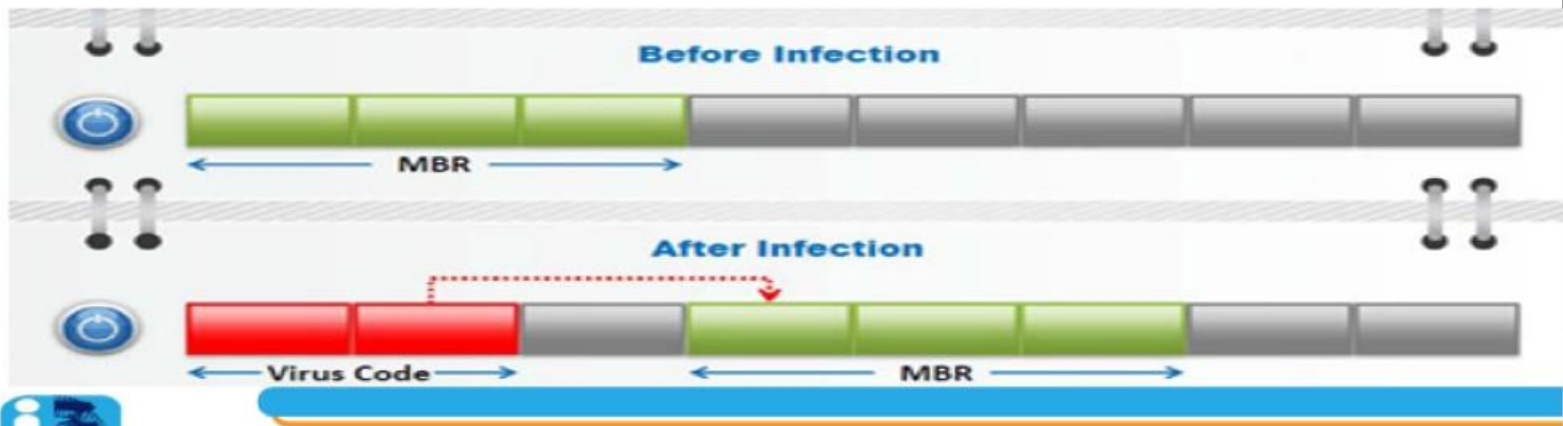


- Infection Phase : the virus replicates itself and attaches to an ---.exe file in the system



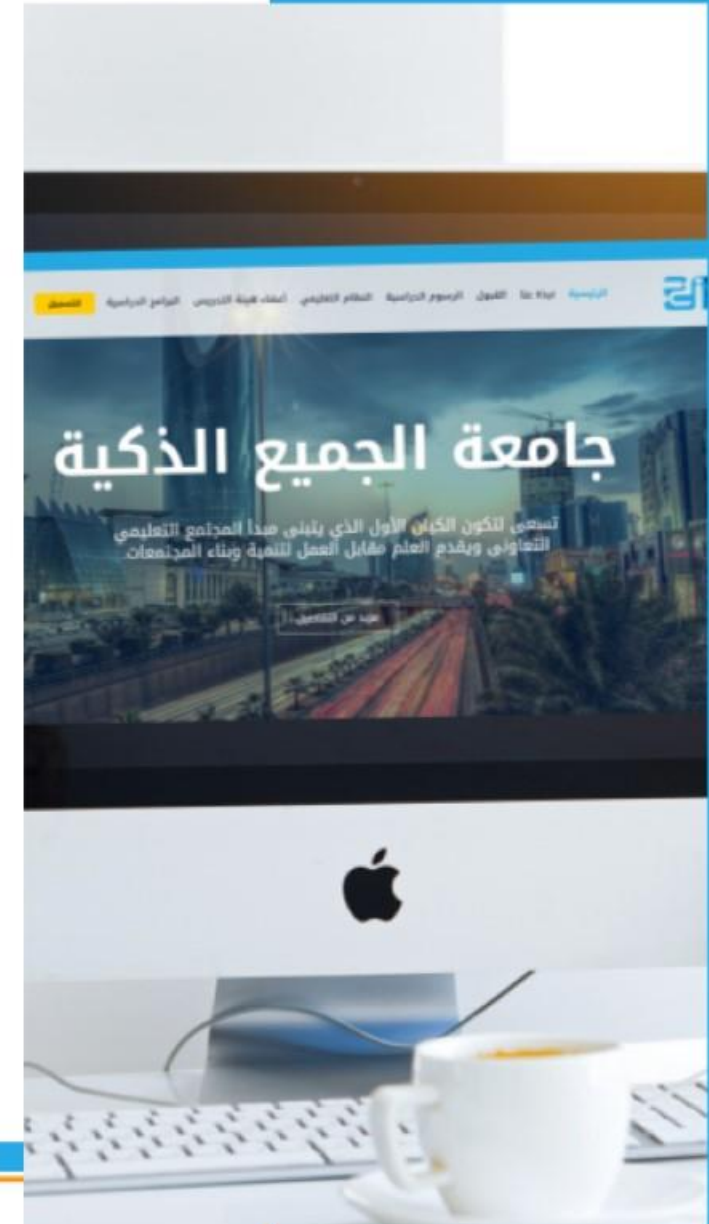
What is a Boot Sector Virus?

- Boot sector viruses are a type of malware that infects a system's boot partition or the master boot record (MBR) of a hard disk. A boot sector is the section of a disk containing the code and data needed to start the operating system (OS) of a computer. While the computer is starting up and before security software is engaged, the virus executes its malicious code.



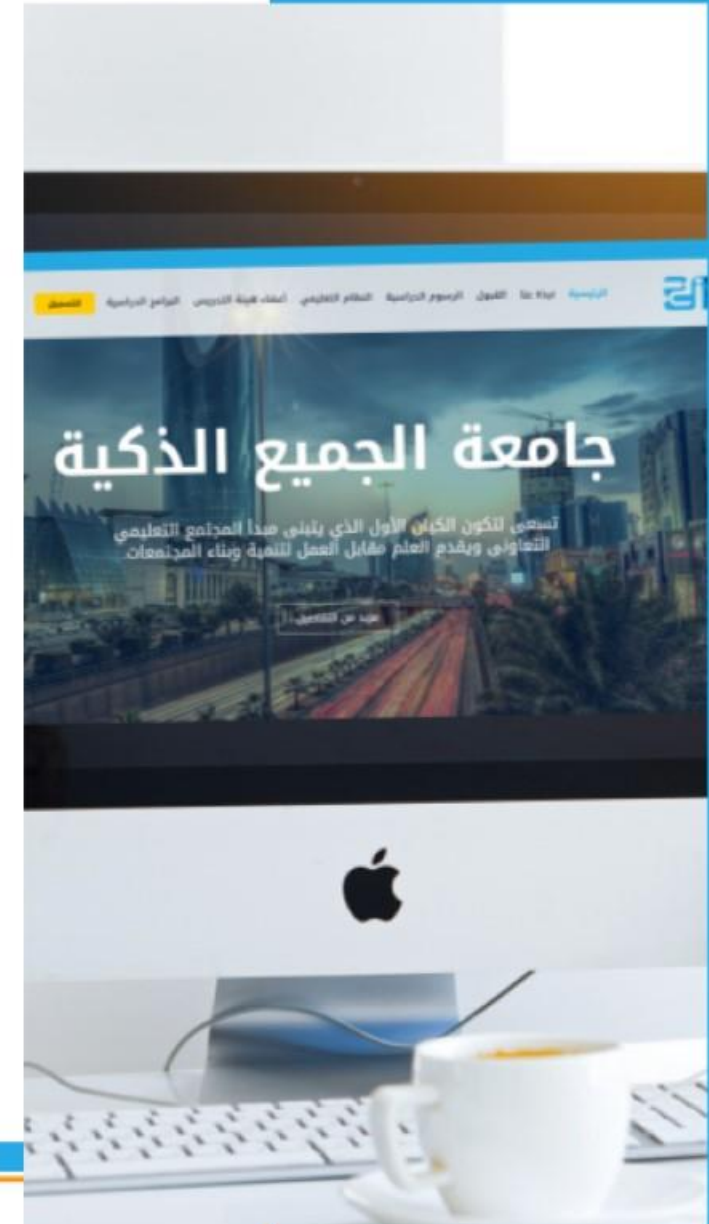
How do Computers become Infected?

- The MBR is on the first sector of your hard drive and executes whenever you power up your computer. This means that even if you try to remove boot sector viruses using an antivirus, they get loaded back into your computer's memory on your next boot.
- Originating from your boot sector, these viruses will then spread to all the disks on your computer. This makes boot sector viruses tough to remove.

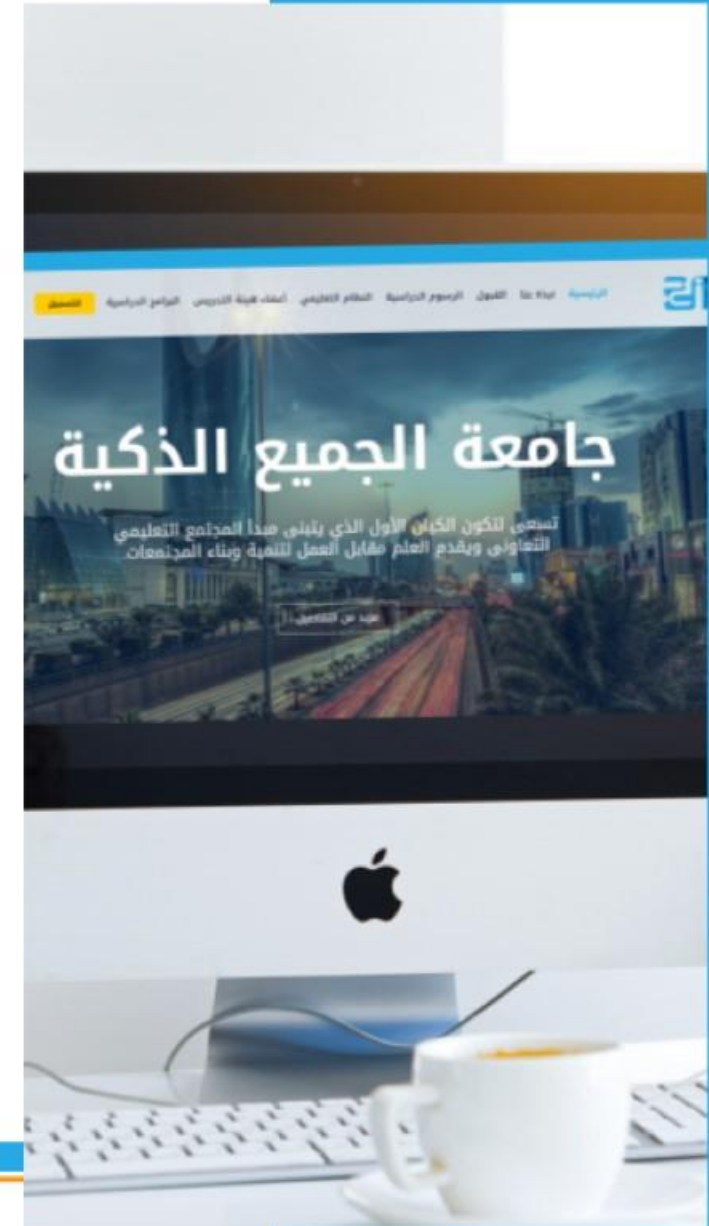


Symptoms of a Boot Sector Virus

- Users are unlikely to know if they have a boot sector virus until they run an antivirus solution or conduct a malware scan. There are a few different signs that a computer has been infected with a boot sector virus. Here are some examples:
 - Boot sector viruses, like most others, can cause your computer to slow down
 - Boot sector viruses can cause a computer to be unable to boot, it may boot to a blue screen, or the OS will not start, or a black screen with an error message may occur

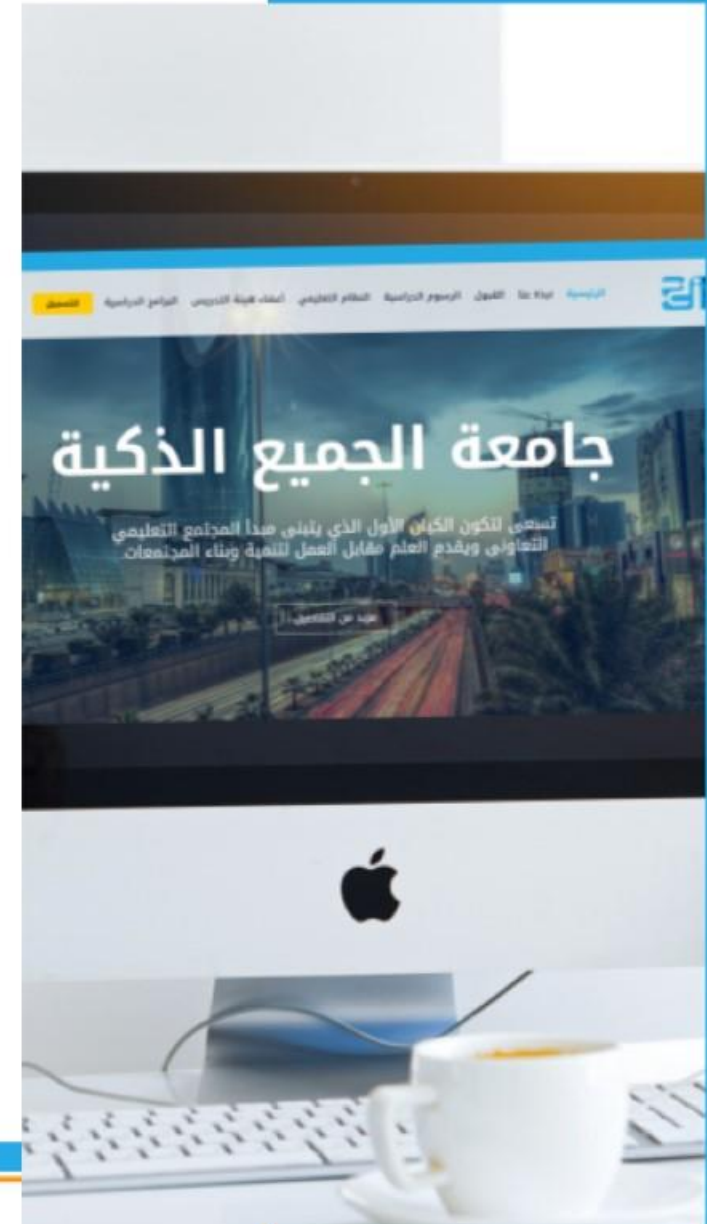


- Use strong, up to date, antivirus software to scan your device for suspicious activity
- When using removable storage devices, such as USB drives, scan it with an antivirus tool before accessing any of the files stored on it
- Avoid using storage devices that you don't know the content of
- Don't download files from emails you weren't expecting

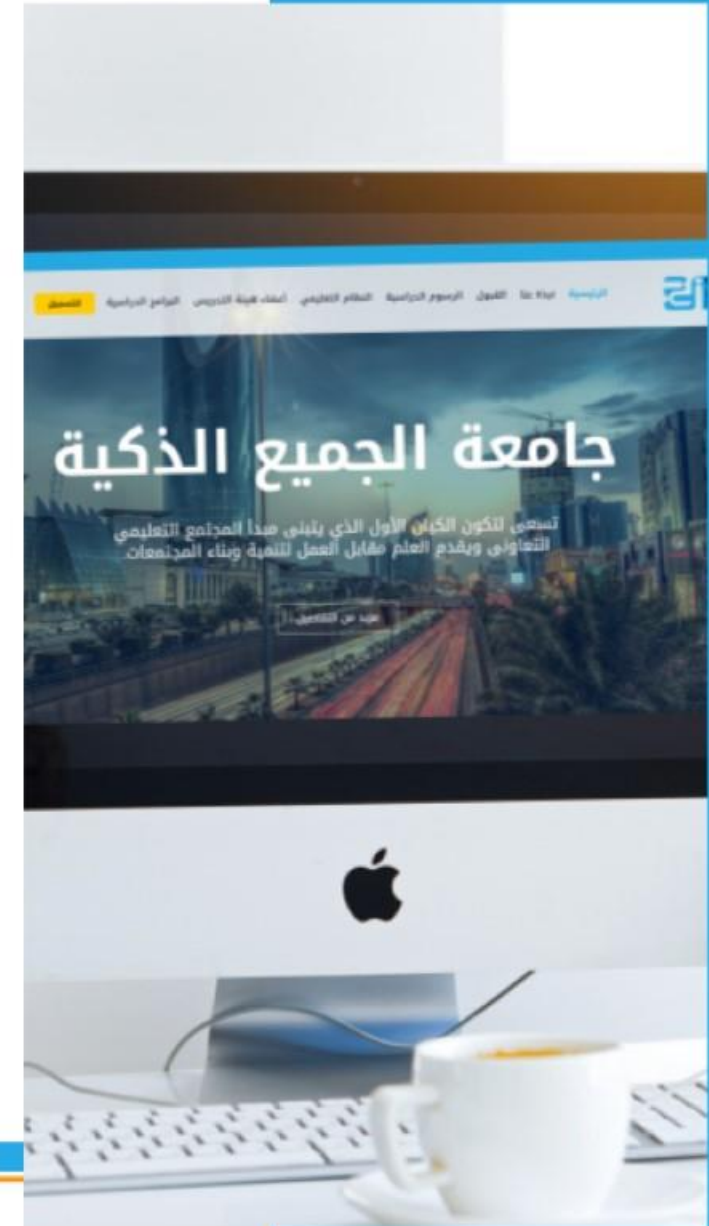


Chapter 04

Ransomware



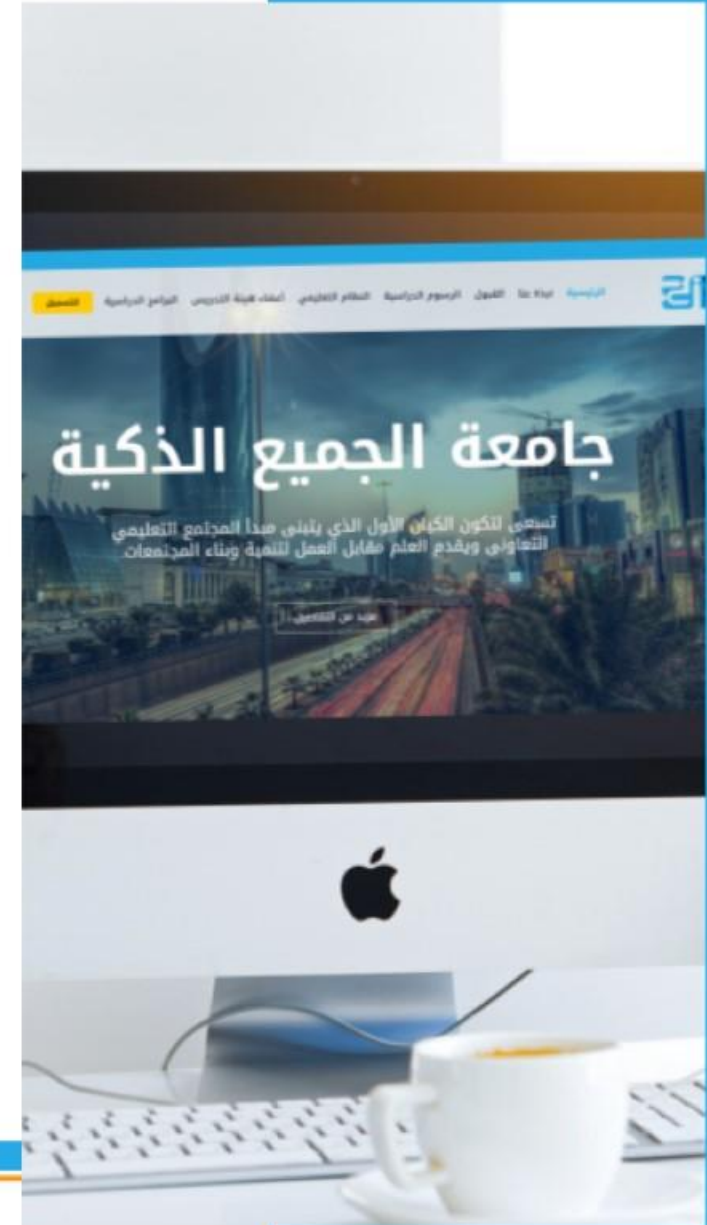
- Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
- While some people might think "a virus locked my computer," ransomware would typically be classified as a different form of malware than a virus. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail.



Chapter 04

Ransomware

- Today, ransomware authors order that payment be sent via cryptocurrency or credit card, and attackers target individuals, businesses, and organizations of all kinds.

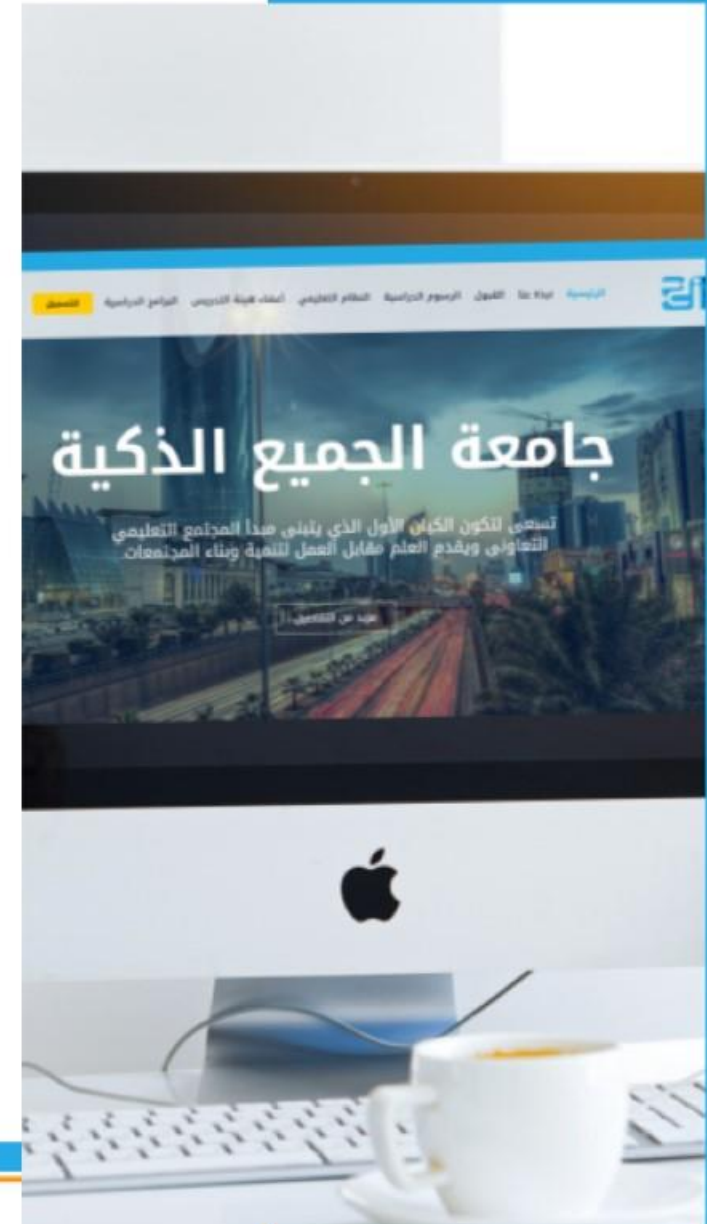


Ransomware attacks

How exactly does a threat actor carry out a ransomware attack?

First, they must gain access to a device or network. Having access enables them to utilize the malware needed to encrypt, or lock up, your device and data.

There are several different ways that ransomware can infect your computer

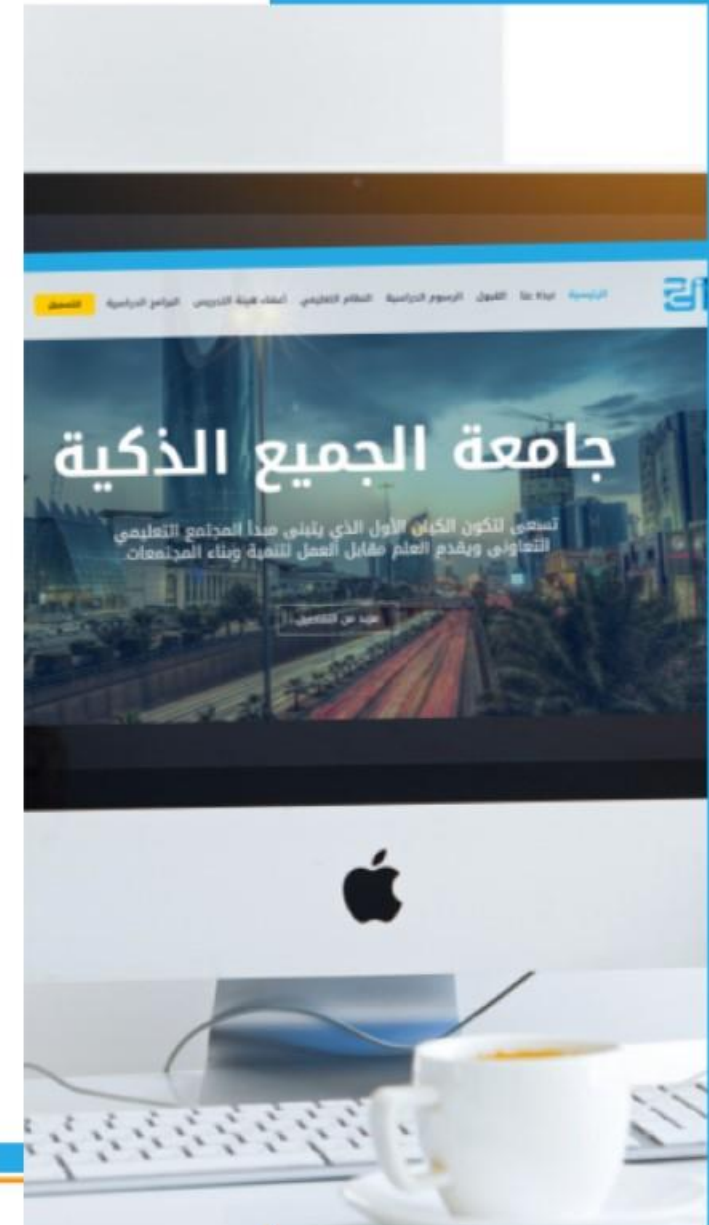


Types of ransomware

Three main types of ransomware include scareware, screen lockers, and encrypting ransomware:

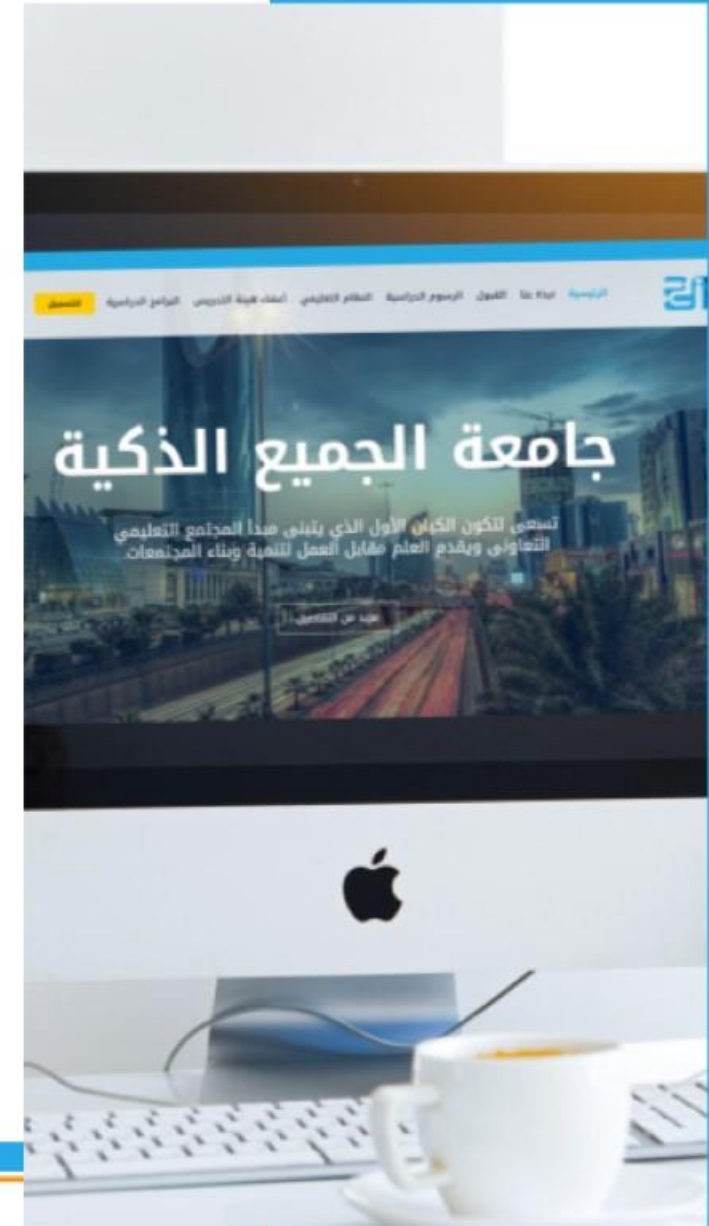
- **Scareware:**

It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up.



Screen lockers:

When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine. However, the FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

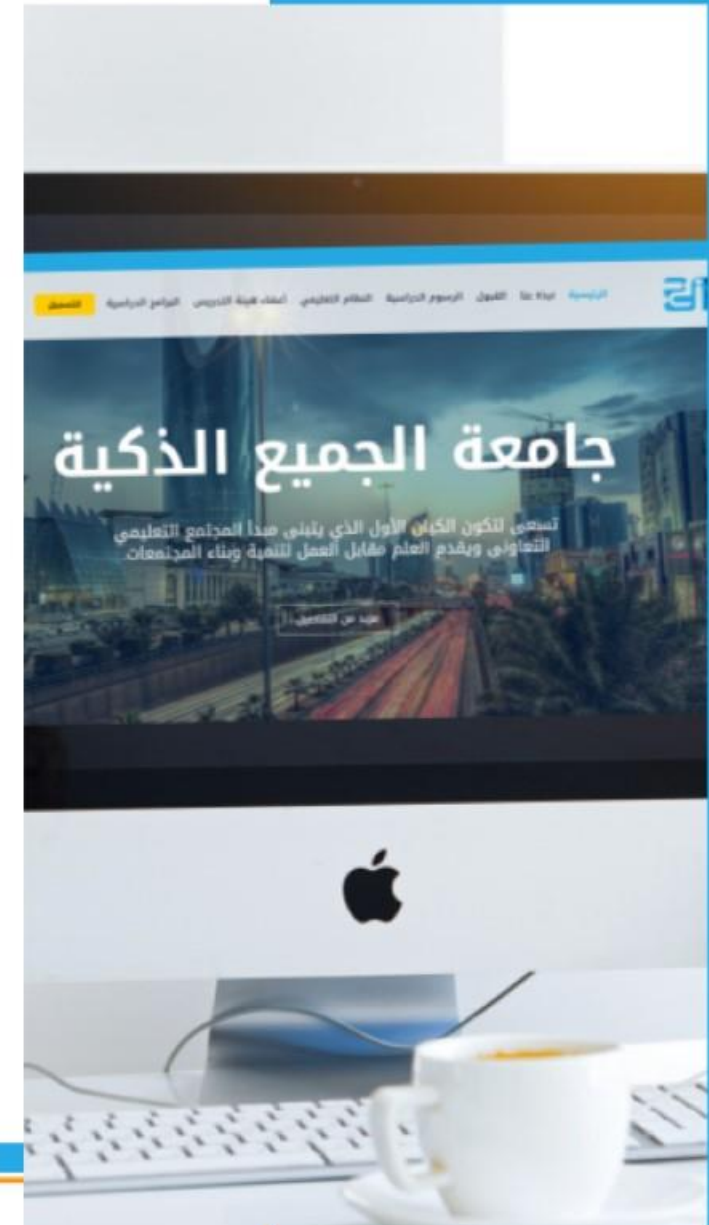


Encrypting ransomware:

These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver.

The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you.

Unless you pay the ransom—for the most part, they're gone. And even if you do pay up, there's no guarantee the cybercriminals will give you those files back.



Chapter 04

Outlines

- <https://www.comparitech.com/ransomware-attack-map/>

Database of US ransomware attacks

Where possible, we have only included ransomware attacks that have been publicly confirmed.

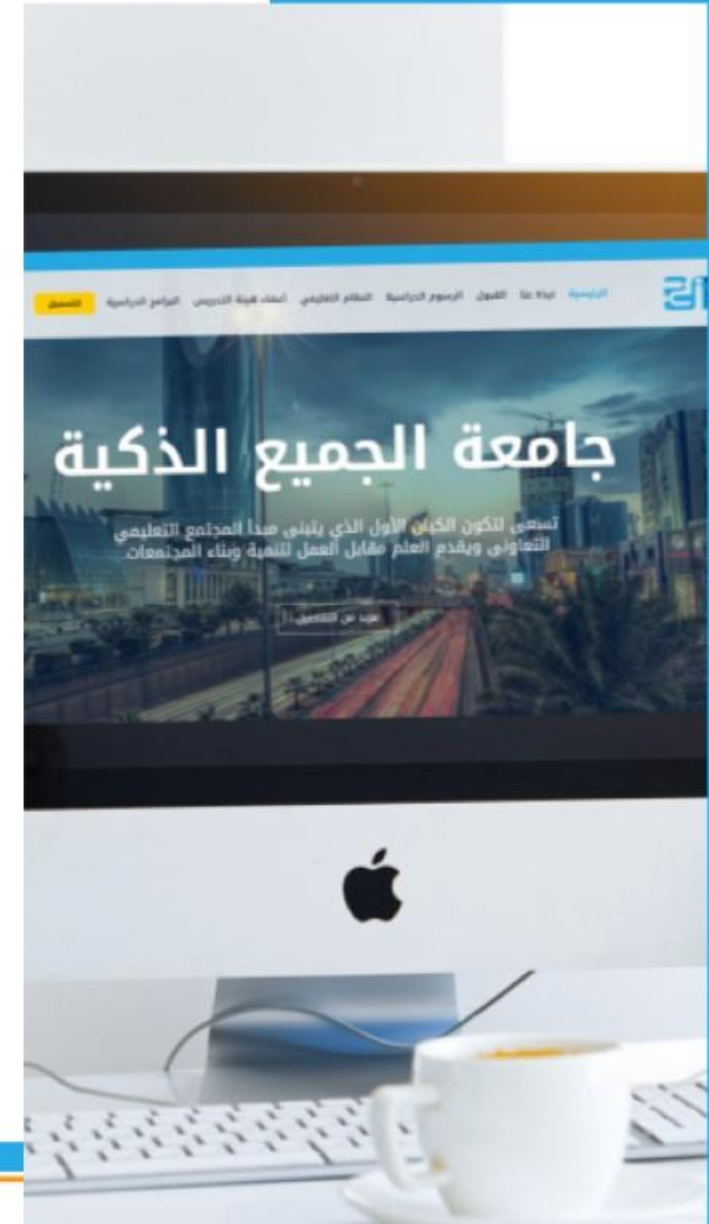
🔍 Search in table

Page 1 of 108 >

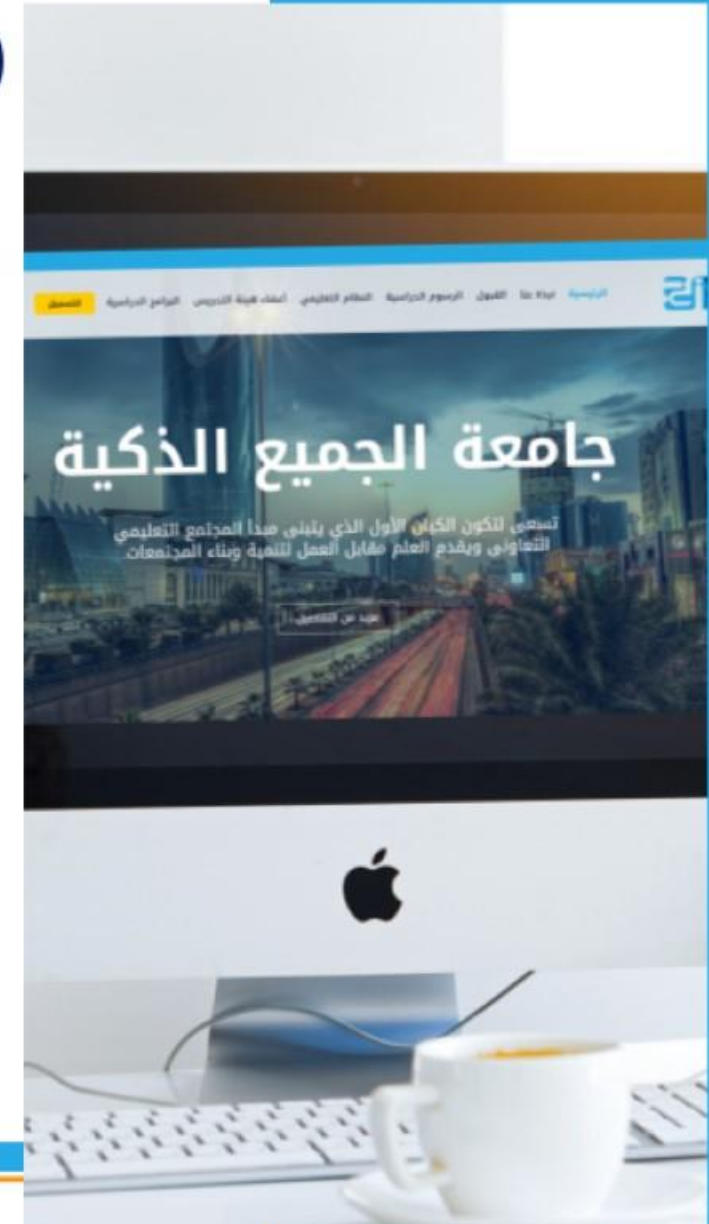
Year	Month, Year ▾	Company Affected	Industry	Sub-Industry	City/County	State	# Records Affected	Ransom Paid	Ransom Amount	Ransomware Strain
2023	Feb, 2023	Wayne County Police Agencies (multiple)	Government	Government	Detroit	Michigan	Unknown	Unknown	Unknown	Unknown
2023	Feb, 2023	MKS Instruments, Inc.	Business	Manufacturing	Andover	Massachusetts	Unknown	Unknown	Unknown	Unknown
2023	Feb, 2023	Hidalgo County Adult Probation Office	Government	Government	Edinburg	Texas	Unknown	Unknown	Unknown	Unknown
2023	Feb, 2023	Berkeley County Public Schools	Education	Education	Martinsburg	West Virginia	Unknown	Unknown	Unknown	Unknown
2023	Feb, 2023	Modesto Police Department	Government	Government	Modesto	California	Unknown	Unknown	Unknown	Unknown
2023	Feb, 2023	City of Oakland	Government	Government	Oakland	California	Unknown	Unknown	Unknown	Unknown
2023	Feb, 2023	Florida Supreme Court	Government	Government	Tallahassee	Florida	Unknown	Unknown	Unknown	Unknown



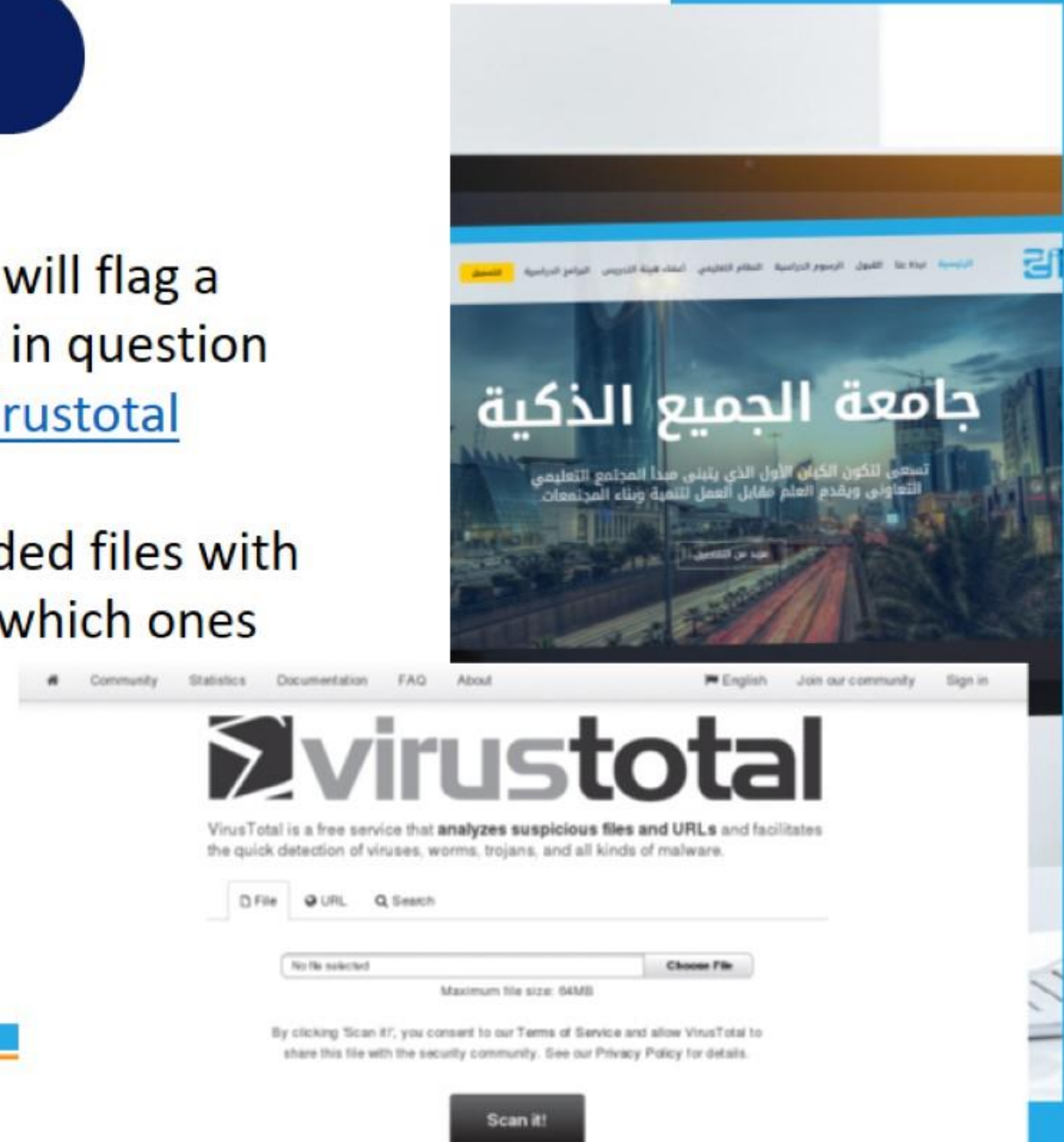
- Most antivirus solutions start by comparing potentially dangerous code to a set of patterns and rules that make up the antivirus definitions, which match known malicious code.
- Antivirus definitions are updated regularly as new malware is identified by each vendor.
- This sort of identification is called **static analysis**.



- In addition to static analysis against a set of signatures, more advanced antivirus solutions also test for malicious activity, called **dynamic analysis**.
- For example, a program that tries to replace every file on the hard drive or connects to a known botnet command and control server every 30 seconds is exhibiting potentially malicious activity and may be flagged.



- One way to see which antivirus solutions will flag a program as malicious is to upload the file in question to the VirusTotal website (<https://www.virustotal.com/>).
- As of this writing, VirusTotal scans uploaded files with about 51 antivirus programs and reports which ones detect malware



Chapter 04

Outlines



SHA256: 5a261239fe890e43d800afe373cff0733b51c98bea04a09d76cd75cb1c7ea7c7

File name: radmin.exe

Detection ratio: 25 / 51

Analysis date: 2014-03-24 04:58:44 UTC (1 minute ago)



Analysis File detail Additional information Comments Votes Behavioural information

Antivirus	Result	Update
AVG	Win32/Patched.IA	20140324
Ad-Aware	Backdoor.Shell.AC	20140324
AntiVir	TR/Crypt.EPACK.Gen2	20140324

Chapter 04

Any Questions

