

# BACKDOOR - TROJAN VIRUS – WORM

9/18/2024

ThS. Nguyễn Duy  
duyn@uit.edu.vn

# Nội Dung

2

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- Cách phát hiện và đối phó Trojan
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- Phân loại Virus
- Worm máy tính
- Cách phát hiện Virus

# Nội Dung

3

duyn@uit.edu.vn

- **Tổng quan về Trojan**
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- Cách phát hiện và đối phó Trojan
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- Phân loại Virus
- Worm máy tính
- Cách phát hiện Virus

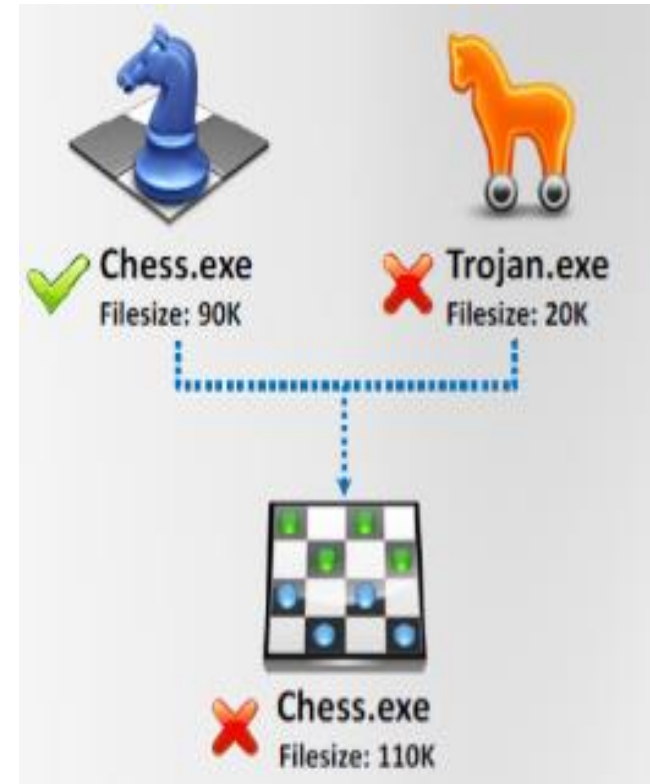
# Tổng quan về Trojan

## Khái niệm

4

duyn@uit.edu.vn

- Là chương trình máy tính có chứa mã độc hại, thường ẩn mình dưới dạng một chương trình hữu ích để chiếm quyền điều khiển, gây thiệt hại đến nạn nhân hay máy tính nạn nhân.
- Trojan có thể nhân bản, lây lan và được kích hoạt bởi những hành động đã được định nghĩa trước.

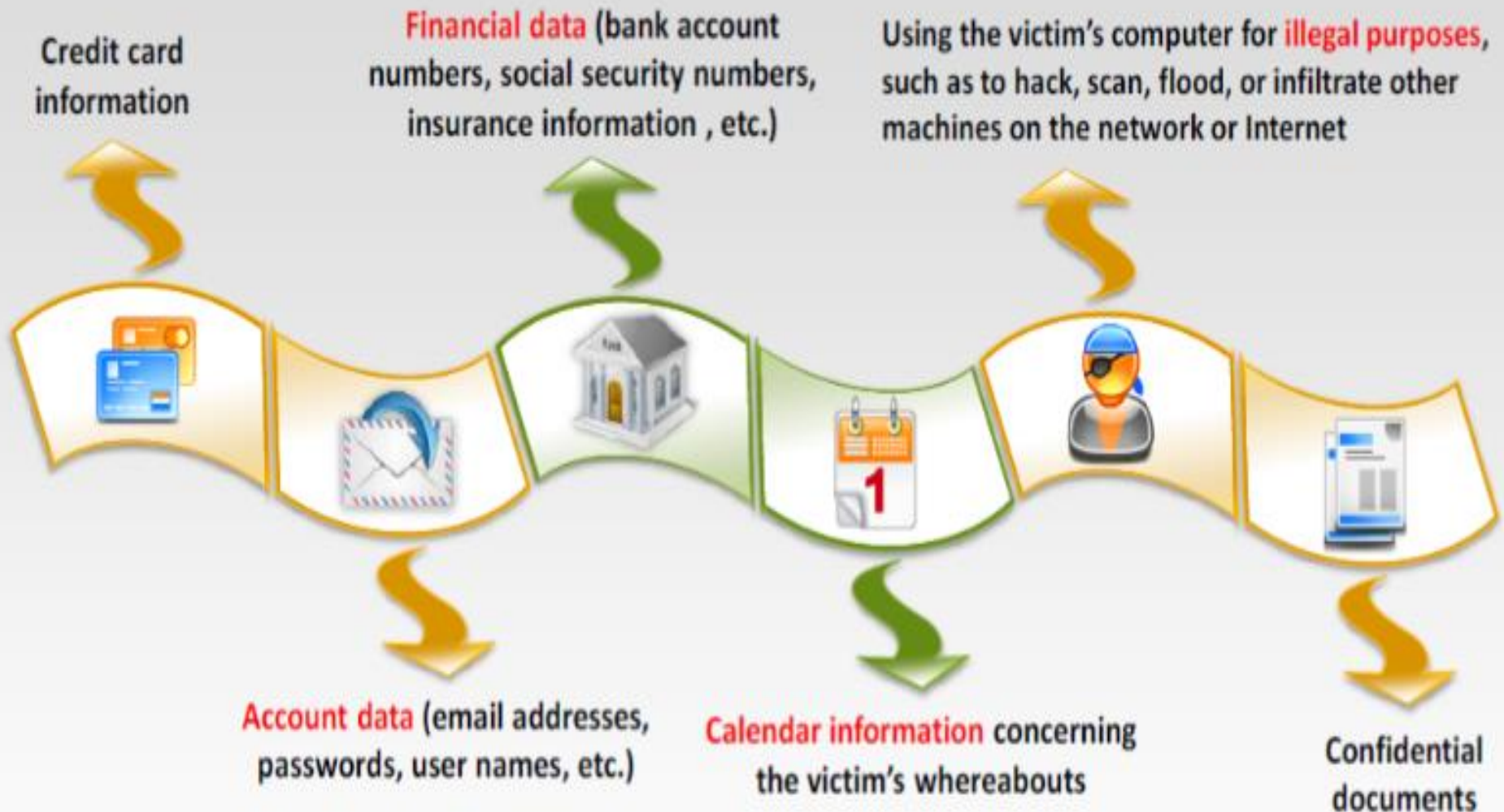


# Tổng quan về Trojan

## Mục đích của Người tạo ra Trojan

5

duyn@uit.edu.vn



# Tổng quan về Trojan

## Mục đích của Trojan

6

duyn@uit.edu.vn



Delete or replace **operating system's critical files**

Disable **firewalls** and **antivirus**



Generate **fake traffic** to create DOS attacks

Create **backdoors** to gain remote access



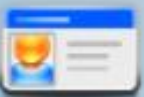
Download **spyware**, **adware**, and malicious files

Infect victim's PC as a **proxy server** for relaying attacks



Record **screenshots**, **audio**, and **video** of victim's PC

Use victim's PC as a **botnet** to perform DDoS attacks



Steal information such as **passwords**, **security codes**, credit card information using keyloggers

Use victim's PC for **spamming** and **blasting email messages**





# Tổng quan về Trojan

## Những dấu hiệu tấn công bởi Trojan

7

duyn@uit.edu.vn



**CD-ROM drawer** opens and closes by itself



Abnormal activity by the **modem**, **network adapter**, or **hard drive**



Computer browser is redirected to **unknown pages**



The account passwords are changed or **unauthorized access**



Strange **chat boxes** appear on victim's computer



Strange **purchase statements** appear in the credit card bills



**Documents** or **messages** are printed from the printer themselves



The **ISP complains** to the victim that his/her computer is IP scanning



Functions of the right and left **mouse buttons** are reversed



People know too much **personal information** about a victim

# Tổng quan về Trojan

## Những dấu hiệu tấn công bởi Trojan - tt

8

duyn@uit.edu.vn





# Tổng quan về Trojan

## Những Port phổ biến Trojan sử dụng

9

duyn@uit.edu.vn

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

# Nội Dung

10

duyn@uit.edu.vn

- Tổng quan về Trojan
- **Quá trình lây nhiễm Trojan**
- Phân loại Trojan
- Cách phát hiện và đối phó Trojan
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- Phân loại Virus
- Worm máy tính
- Cách phát hiện Virus

# Quá trình lây nhiễm Trojan

11

duyn@uit.edu.vn





# Phương pháp trốn tránh Anti-Virus của Trojan

12

duyn@uit.edu.vn



Never use Trojans downloaded from the **web** (antivirus can detect these easily)



Break the Trojan file into **multiple pieces** and zip them as **single file**

**ALWAYS** write your own Trojan and embed it into an application

Change the content of the Trojan using **hex editor** and also change the **checksum** and encrypt the file

**Change Trojan's syntax:**

- Convert an EXE to VB script
- Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)

# Nội Dung

13

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- **Phân loại Trojan**
- Cách phát hiện và đối phó Trojan
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- Phân loại Virus
- Worm máy tính
- Cách phát hiện Virus



# Phân loại Trojan

14

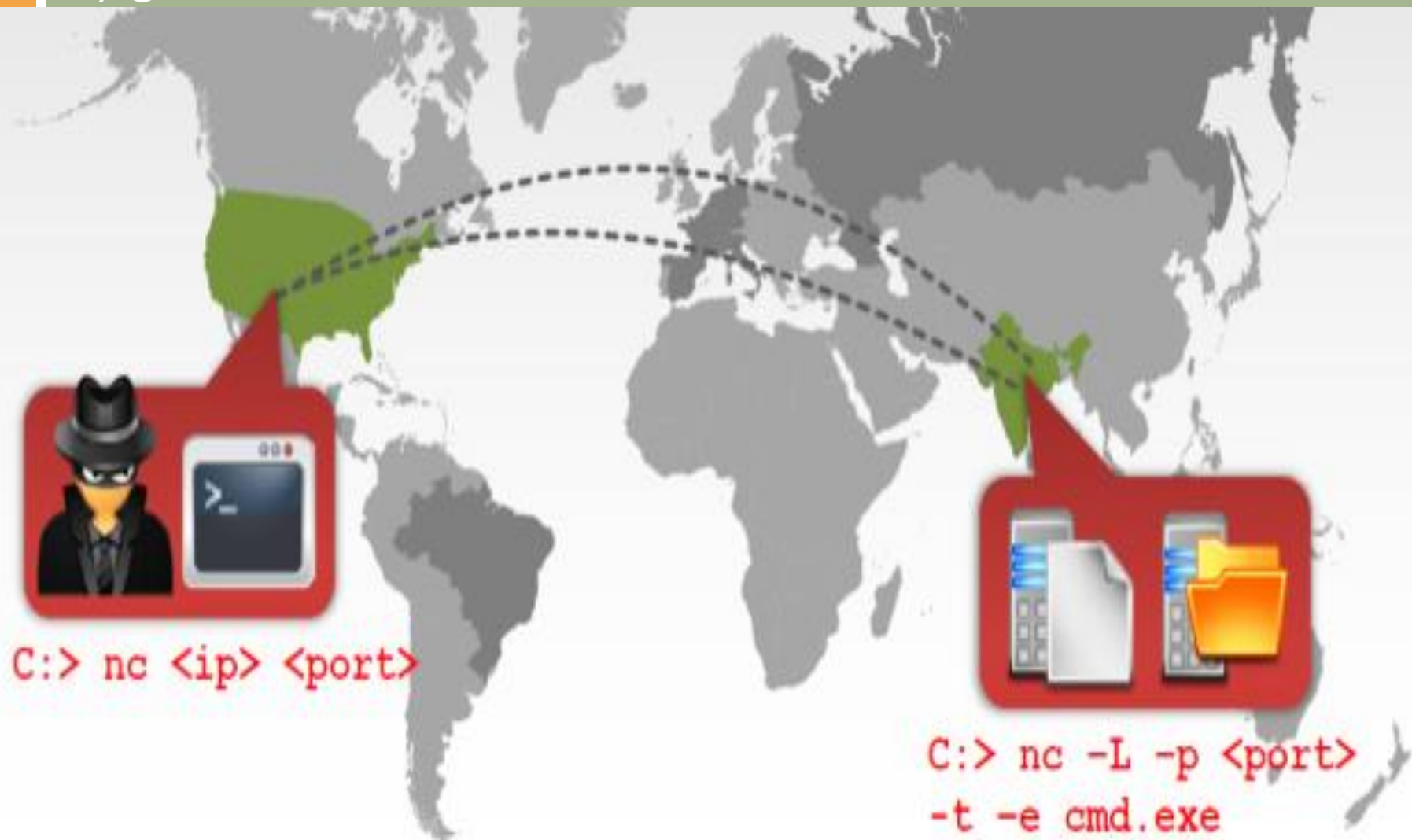
duyn@uit.edu.vn



# Command Shell Trojan

15

duyn@uit.edu.vn



# Document Trojan

16

duyn@uit.edu.vn

VIA LETTER

John Stevens  
Royal Communications Company  
445 152<sup>th</sup> Street S.W.  
Washington, DC 20554



September 2, 2012

RE: Fedex Shipment Airway Bill Number: 867676340056

Dear Mr. Stevens:

We have received a package addressed to you at the value of USD 2,300. The custom duty has not been paid for this shipment which is listed as Apple iMac 24" Computer.

Please call us at Fedex at 1800-234-446 Ext 345 or e-mail me at [m.roberts@fedex.com](mailto:m.roberts@fedex.com) regarding this shipment.

Please visit our Fedex Package Tracking Website to see more details about this shipment and advice us on how to proceed. The website link is attached with this letter.



Package

**Trojan embedded in Word document**

Sincerely,  
**Michelle Roberts**  
Customer Service Representative  
International Shipment and Handling  
Fedex Atlanta Division  
Tel: 1800-234-446 Ext 345  
<http://www.fedex.com>  
[m.roberts@fedex.com](mailto:m.roberts@fedex.com)





# Email Trojan

17

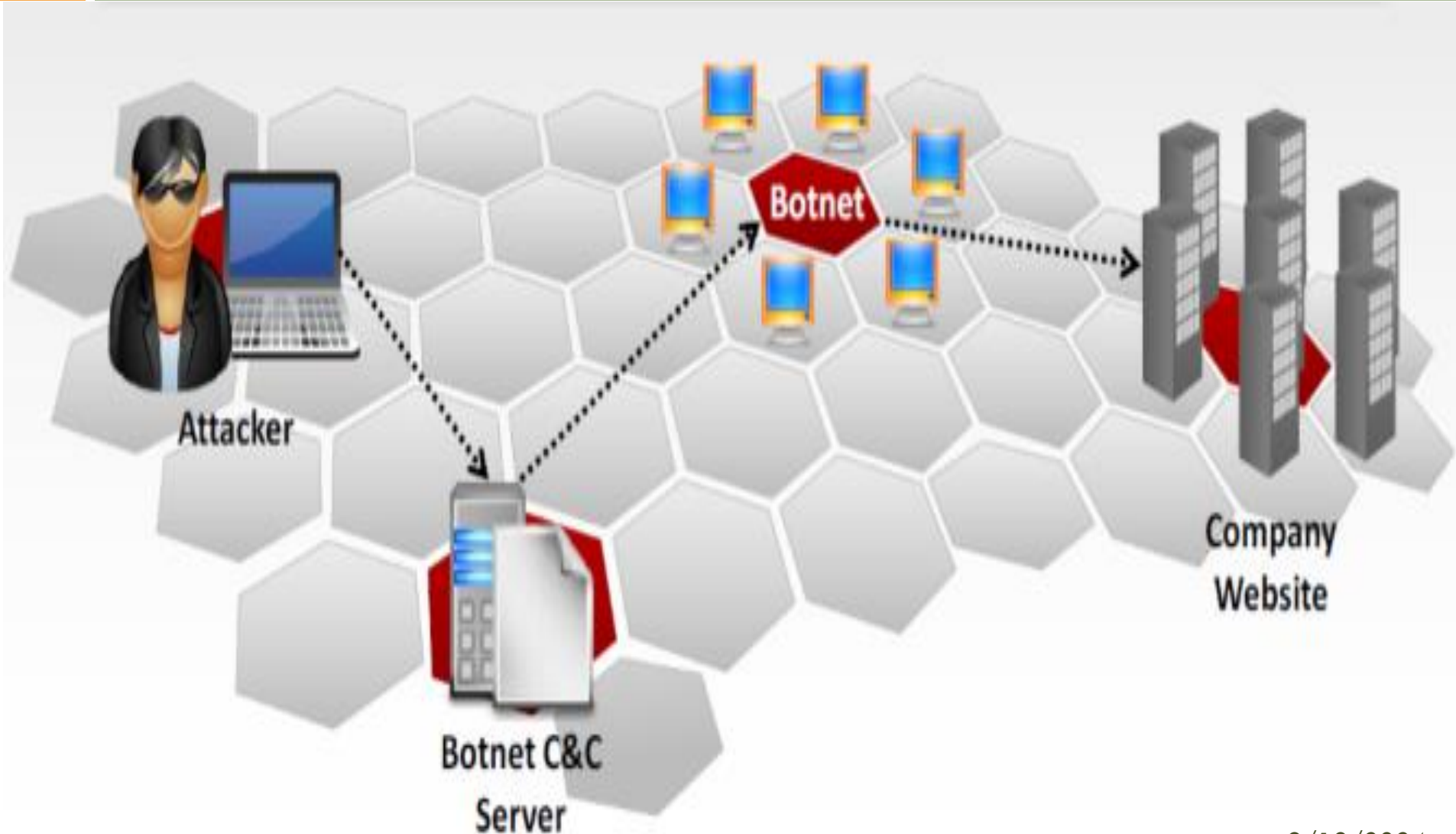
duyn@uit.edu.vn



# Botnet Trojan

18

duyn@uit.edu.vn





# Proxy Trojan

19

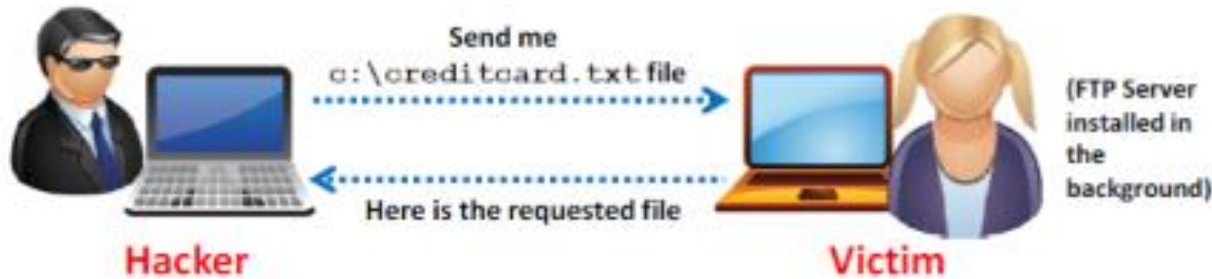
duyn@uit.edu.vn



# FTP Trojan

20

duyn@uit.edu.vn



## FTP Trojan: TinyFTPD

- FTP Trojans install an **FTP server** on the victim's machine, which opens **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

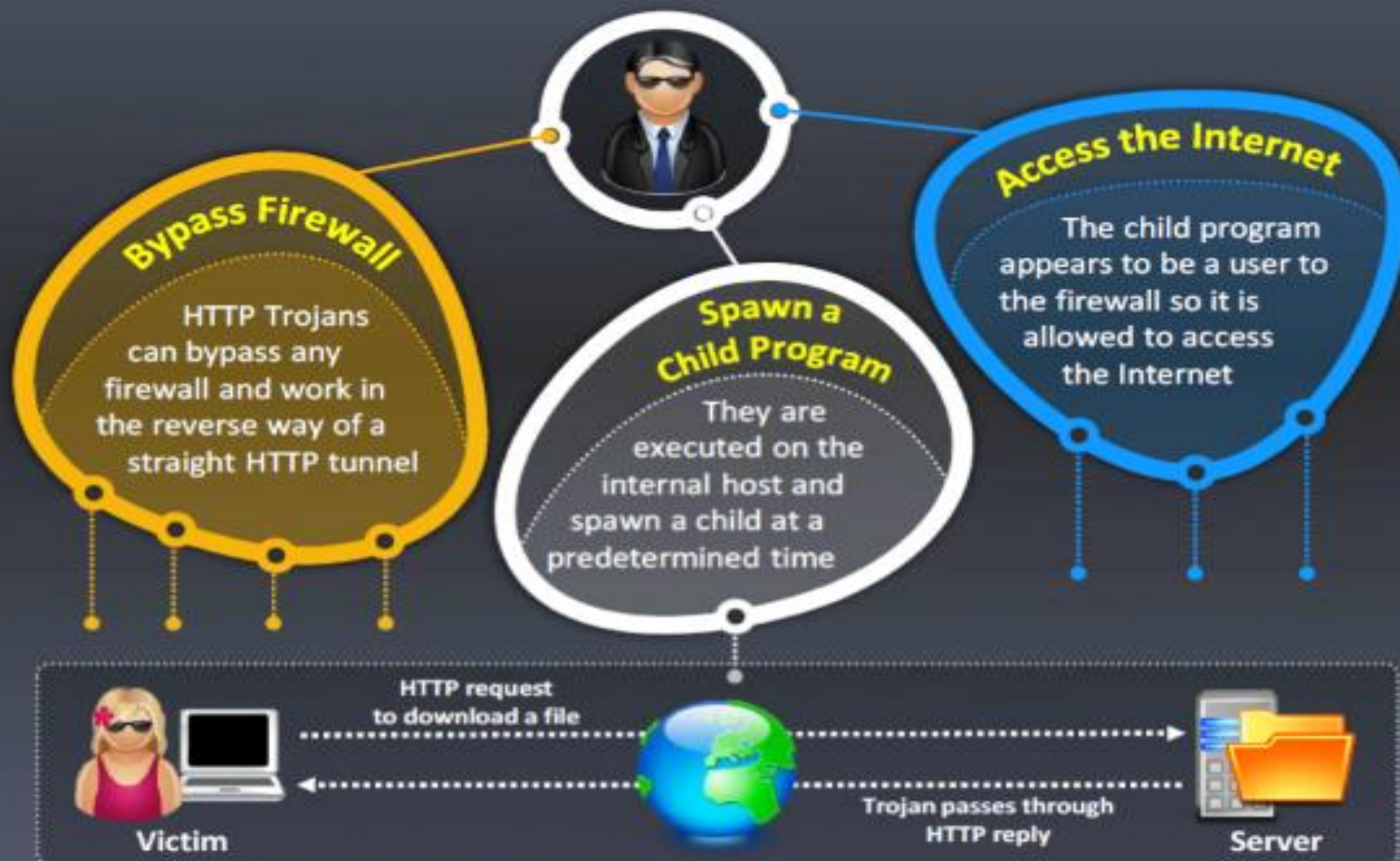


```
C:\Documents and Settings\Admin\Desktop>TinyFTPD 21 5555 test test c:\win98 all RMLCD
Tiny FTPD V1.4 By WinEggDrop
FTP Server Is Started
ControlPort: 21
BindPort: 55555
UserName: test
Password: test
HomeDir: c:\win98
Allow IP: all
Local Address: 192.168.168.16
ReadAccess: Yes
WriteAccess: Yes
ListAccess: Yes
CreateAccess: Yes
DeleteAccess: Yes
ExecuteAccess: Yes
UnlockAccess: No
AnonymousAccess: No
Check Time Out Thread Created Successfully
***** Waiting For New Connection *****
0 Connection Is In Use
```

# HTTP Trojan

21

duyn@uit.edu.vn





# Remote Access Trojan (RAT)

22

duyn@uit.edu.vn



- This Trojan works like a **remote desktop access**
- Hacker gains complete **GUI access** to the remote system

1. Infect (Rebecca's) computer with **server.exe** and plant Reverse Connecting Trojan
2. The Trojan connects to **Port 80** to the attacker in Russia establishing a reverse connection
3. Jason, the attacker, has complete **control** over Rebecca's machine



# Nội Dung

23

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- **Cách phát hiện và đối phó Trojan**
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- Phân loại Virus
- Worm máy tính
- Cách phát hiện Virus



# Cách phát hiện và đối phó Trojan

24

duyn@uit.edu.vn



Scan for suspicious **OPEN PORTS**



Scan for suspicious **RUNNING PROCESSES**



Scan for suspicious **REGISTRY ENTRIES**



Scan for suspicious **DEVICE DRIVERS**  
installed on the computer



Scan for suspicious **WINDOWS SERVICES**



Scan for suspicious **STARTUP PROGRAMS**



Scan for suspicious **FILES** and **FOLDERS**



Scan for suspicious **NETWORK ACTIVITIES**



Scan for suspicious modification to  
**OPERATING SYSTEM FILES**



Run Trojan **SCANNER** to detect Trojans



# Cách phát hiện và đối phó Trojan Quét Port

25

duyn@uit.edu.vn

- Trojans open **unused ports** in victim machine to connect back to Trojan handlers
- Look for the **connection established** to unknown or suspicious IP addresses



```
C:\Windows\system32\cmd.exe

C:\Users\Admin>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135               0.0.0.0:0               LISTENING
TCP    0.0.0.0:445               0.0.0.0:0               LISTENING
TCP    0.0.0.0:554               0.0.0.0:0               LISTENING
TCP    0.0.0.0:1025              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1026              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1027              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1028              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1029              0.0.0.0:0               LISTENING
TCP    0.0.0.0:2069              0.0.0.0:0               LISTENING
TCP    0.0.0.0:5357              0.0.0.0:0               LISTENING
TCP    0.0.0.0:10243             0.0.0.0:0               LISTENING
TCP    0.0.0.0:22350             0.0.0.0:0               LISTENING
TCP    127.0.0.1:12025            0.0.0.0:0               LISTENING
TCP    127.0.0.1:12000            0.0.0.0:0               LISTENING
TCP    127.0.0.1:12000            127.0.0.1:53050         ESTABLISHED
TCP    127.0.0.1:12000            127.0.0.1:53052         ESTABLISHED
TCP    127.0.0.1:12110            0.0.0.0:0               LISTENING
```

Type **netstat -an**  
in command prompt



System Administrator

# Cách phát hiện và đối phó Trojan Quét Process

26

duyn@uit.edu.vn

Process Monitor is a monitoring tool for **Windows** that shows file system, registry, and process/thread activity

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result
11:09:...	Explorer.EXE	5572	CreateFileMa...	C:\Program Files (x86)\Mozilla Firefo...	SUCCESS
11:09:...	Explorer.EXE	5572	RegOpenKey	HKLM\Software\Microsoft\Window...	SUCCESS
11:09:...	Explorer.EXE	5572	RegQueryValue	HKLM\SOFTWARE\Microsoft\Win...	NAME NO
11:09:...	Explorer.EXE	5572	RegCloseKey	HKLM\SOFTWARE\Microsoft\Win...	SUCCESS
11:09:...	Explorer.EXE	5572	CreateFile	C:\Program Files (x86)\Mozilla Firefo...	NAME NO
11:09:...	Explorer.EXE	5572	QueryBasicInf...	C:\Program Files (x86)\Mozilla Firefo...	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\sxssrv.dll	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\csrsrv.dll	SUCCESS
11:09:...	csrss.exe	548	RegQueryValue	HKLM\SOFTWARE\Microsoft\Win...	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\sxss.dll	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\sxss.dll	SUCCESS
11:09:...	csrss.exe	548	RegQueryKey	HKLM	SUCCESS

Showing 359,375 of 662,305 events (54%) Backed by virtual memory



# Cách phát hiện và đối phó Trojan Quét Service

27

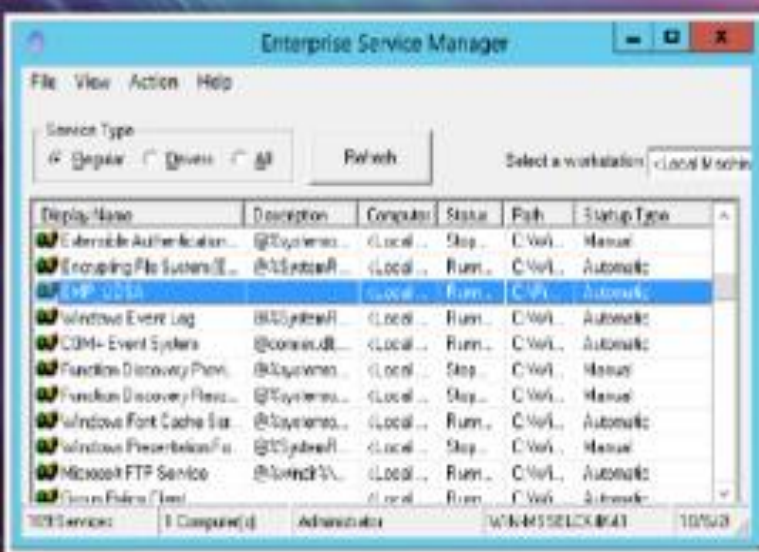
duyn@uit.edu.vn

Trojans spawn **Windows services** allow attackers remote control to the victim machine and pass malicious instructions

Trojans **rename their processes** to look like a genuine Windows service in order to avoid detection



Trojans **employ rootkit techniques** to manipulate `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services` registry keys to hide its processes



# Cách phát hiện và đối phó Trojan

## Quét Startup Program

28

duyn@uit.edu.vn

### Check start up folder

`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`

`C:\Users\ (User-Name) \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

### Check Windows services automatic started

Go to **Run** → Type **services.msc**  
→ Sort by **Startup Type**

### Check start up program entries in the registry

Details are covered in next slide

### Check device drivers automatically loaded

`C:\Windows\System32\drivers`

Check **boot.ini**  
or **bcd** (bootmgr) entries



# Cách phát hiện và đối phó Trojan

29

duyn@uit.edu.vn



# Cách phát hiện và đối phó Backdoor - tt

30

duyn@uit.edu.vn



Most commercial **anti-virus products** can automatically scan and detect **backdoor programs** before they can cause damage



Educate users not to install applications downloaded from **untrusted Internet sites** and **email attachments**



Use **anti-virus tools** such as Windows Defender, McAfee, and Norton to detect and eliminate backdoors

# Anti Trojan Software

31

duyn@uit.edu.vn



**Anti-Trojan Shield (ATS)**

<http://www.atshield.com>



**SPYWAREfighter**

<http://www.spamfighter.com>



**Spyware Doctor**

<http://www.pctools.com>



**Anti Trojan Elite**

<http://www.remove-trojan.com>



**Anti Malware BOClean**

<http://www.comodo.com>



**SUPERAntiSpyware**

<http://www.superantispyware.com>



**Anti Hacker**

<http://www.hide-my-ip.com>



**Trojan Remover**

<http://www.simplysup.com>



**XoftSpySE**

<http://www.paretologic.com>



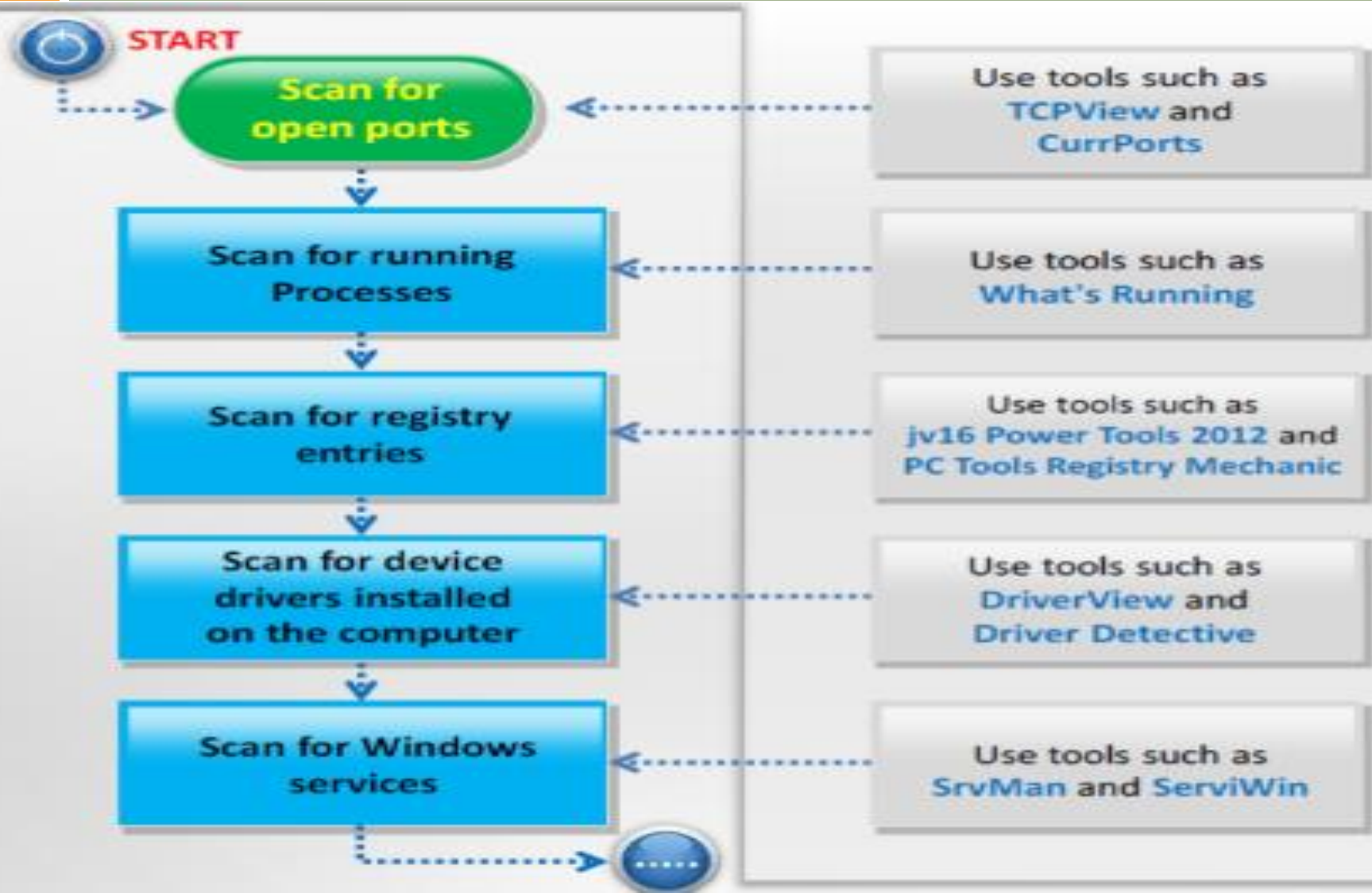
**Twister Antivirus**

<http://www.filseclab.com>

# Quy trình kiểm tra Trojan

32

duyn@uit.edu.vn





# Nội Dung

33

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- Cách phát hiện và đối phó Trojan
- **Khái niệm Virus và Worm**
- Quá trình lây nhiễm Virus
- Phân loại Virus
- Worm máy tính
- Cách phát hiện Virus

# Khái niệm Virus

## Tổng quan

34

duyn@uit.edu.vn

- Là một phần mềm có thể sao chép chính nó. Nó không đứng một mình mà phải gắn vào một tập tin hoặc một chương trình khác.
- Khi một chương trình bị nhiễm virus máy tính được thực hiện hoặc một tập tin bị nhiễm được mở ra, loại virus chứa trong nó sẽ được thực thi.

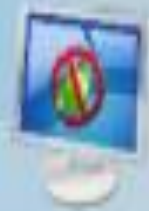
# Khái niệm Virus

## Các đặc điểm của Virus

35

duyn@uit.edu.vn

### Virus Characteristics



Infects Other Program



Transforms Itself



Encrypts Itself



Alters Data



Corrupts Files and Programs



Self Propagates



# Khái niệm Virus

## Những giai đoạn trong chu kỳ sống của Virus

36

duyn@uit.edu.vn



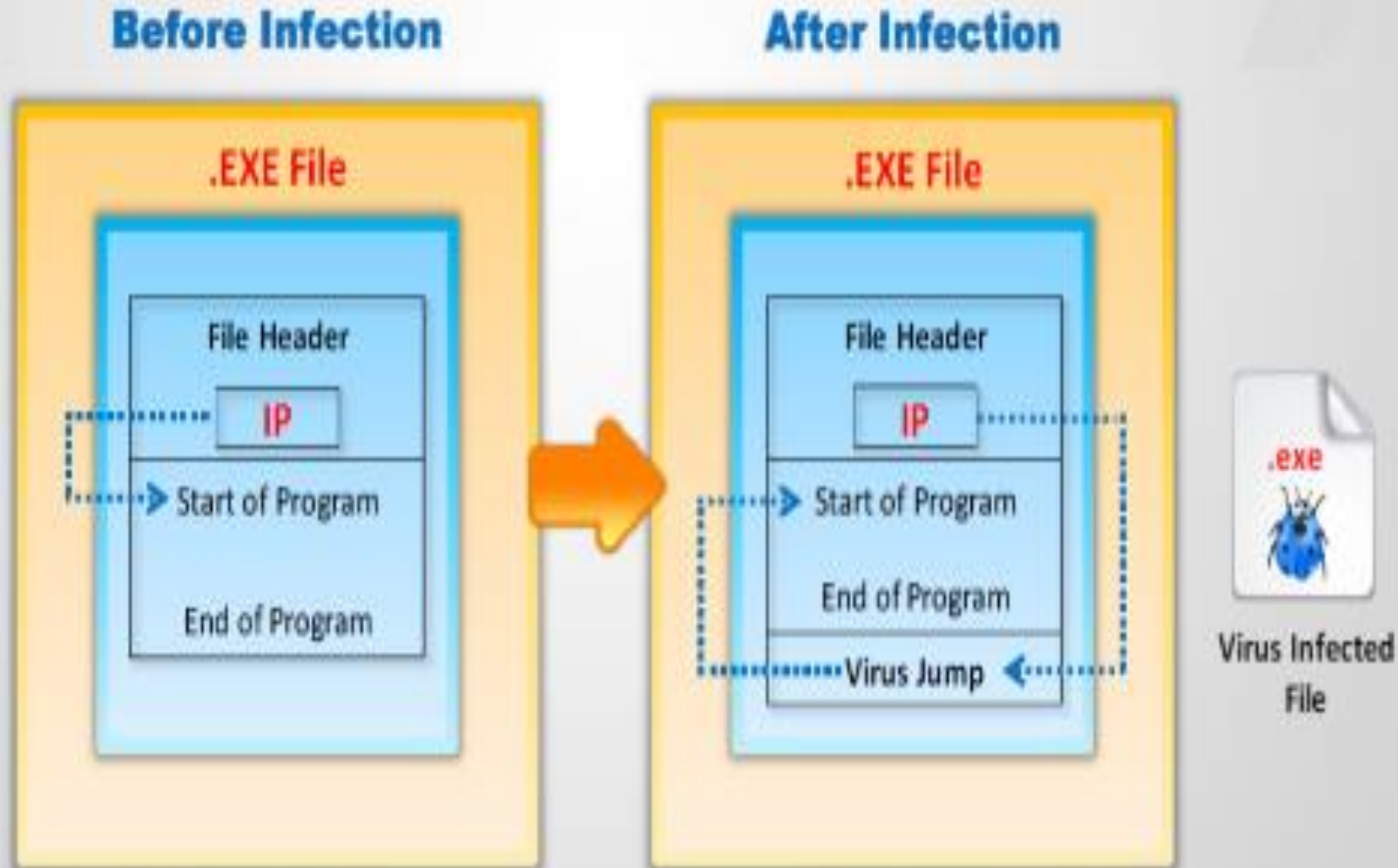


# Khái niệm Virus

## Cơ chế làm việc của Virus

37

duyn@uit.edu.vn



# Khái niệm Virus

## Cơ chế làm việc của Virus

38

duyn@uit.edu.vn

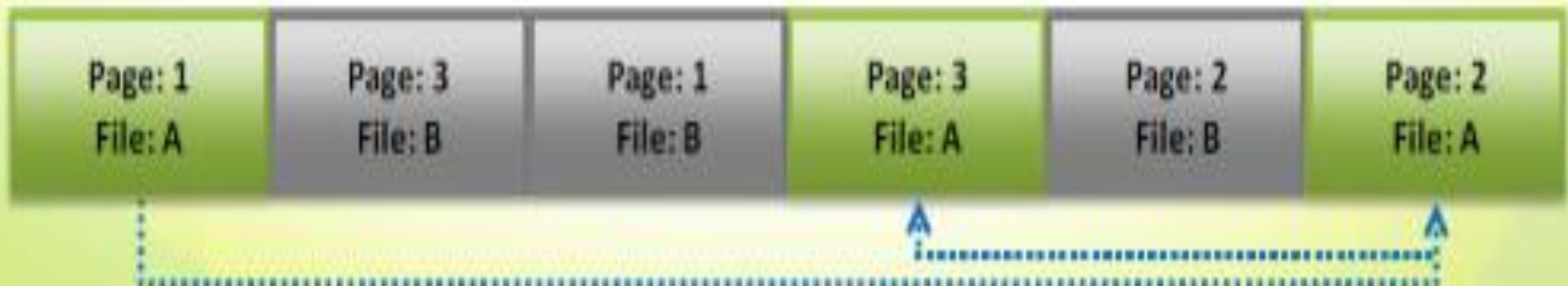
### Unfragmented File Before Attack

File: A

File: B



### File Fragmented Due to Virus Attack



# Khái niệm Virus

## Mục đích của người tạo ra Virus

39

duyn@uit.edu.vn



### Computer Viruses



Inflict damage to competitors



Financial benefits



Research projects



Play prank



Vandalism



Cyber terrorism



Distribute political messages



Attacker



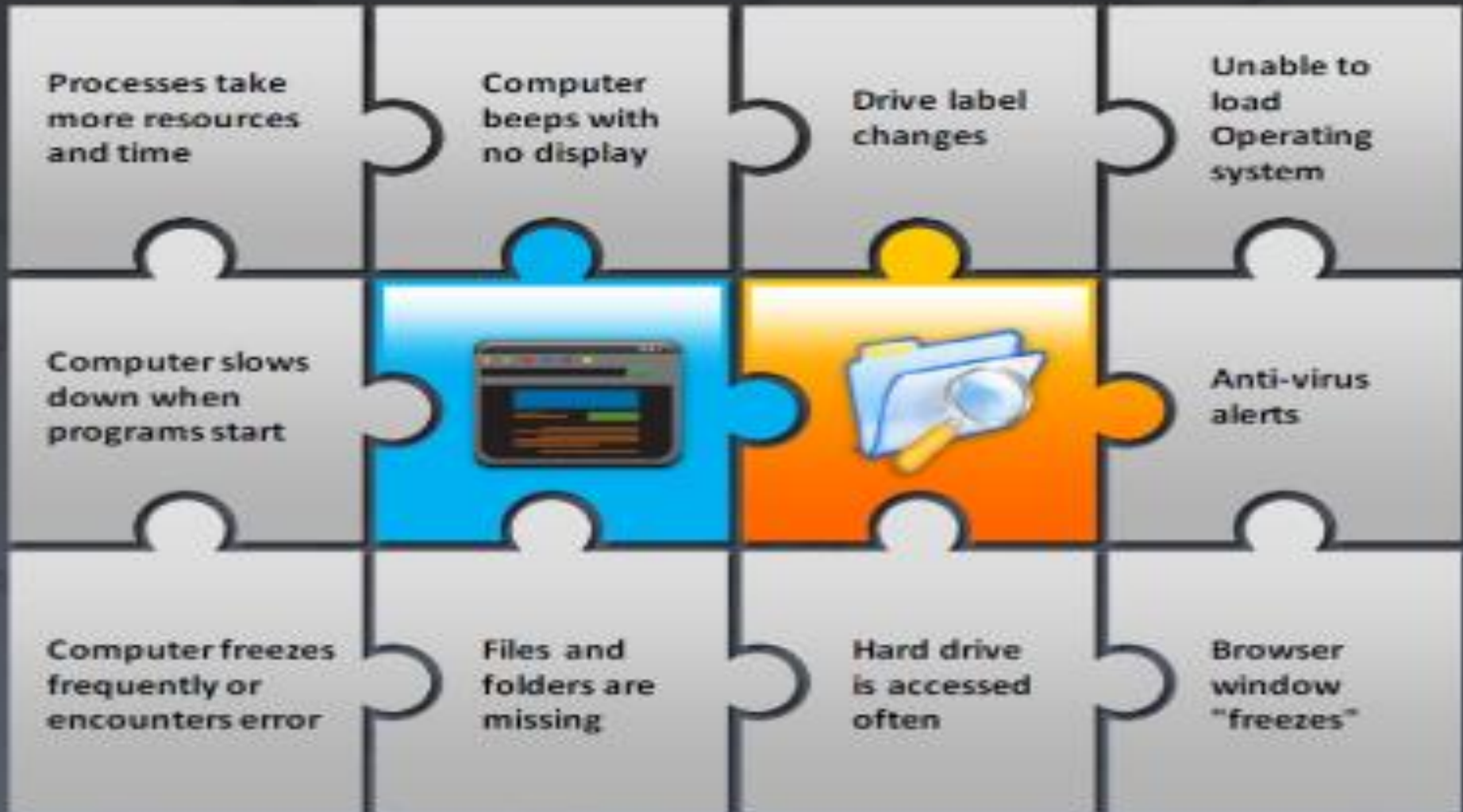
Vulnerable System

# Khái niệm Virus

## Những dấu hiệu bị Virus tấn công

40

duyn@uit.edu.vn





# Nội Dung

41

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- Cách phát hiện Trojan
- Khái niệm Virus và Worm
- **Quá trình lây nhiễm Virus**
- Phân loại Virus
- Worm máy tính
- Cách phát hiện Virus

# Khái niệm Virus

## Quá trình lây nhiễm Virus

42

duyn@uit.edu.vn



When a user accepts files and **downloads without checking** properly for the source



Opening **infected e-mail attachments**



Installing **pirated software**



Not updating and not installing new versions of **plug-ins**



Not running the latest **anti-virus application**

# Nội Dung

43

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- Cách phát hiện Trojan
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- **Phân loại Virus**
- Worm máy tính
- Cách phát hiện Virus

# Nội Dung

## Phân loại Virus

44

duyn@uit.edu.vn





# System or Boot Sector Viruses

du.edu.vn

## Boot Sector Virus

Boot sector virus **moves MBR to another location** on the hard disk and copies itself to the original location of MBR



## Execution

When system boots, **virus code is executed first** and then control is passed to original MBR



## Before Infection



## After Infection



# File and Multipartite Viruses

## File Viruses

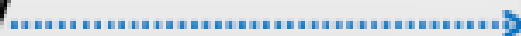
- File viruses infect files which are **executed or interpreted in the system** such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files
- File viruses can be either direct-action (non-resident) or memory-resident

## Multipartite Virus

- Multipartite viruses infect the system **boot sector** and the **executable files** at the same time



**Attacker**



# Macro Viruses

duyn@uit.edu.vn



Attacker



Infests Macro Enabled Documents



User

- Macro viruses **infect files** created by Microsoft Word or Excel



- Most macro viruses are written using **macro language Visual Basic** for Applications (VBA)



- Macro viruses infect **templates** or **convert infected documents into template files**, while maintaining their appearance of ordinary document files

# Encryption Viruses

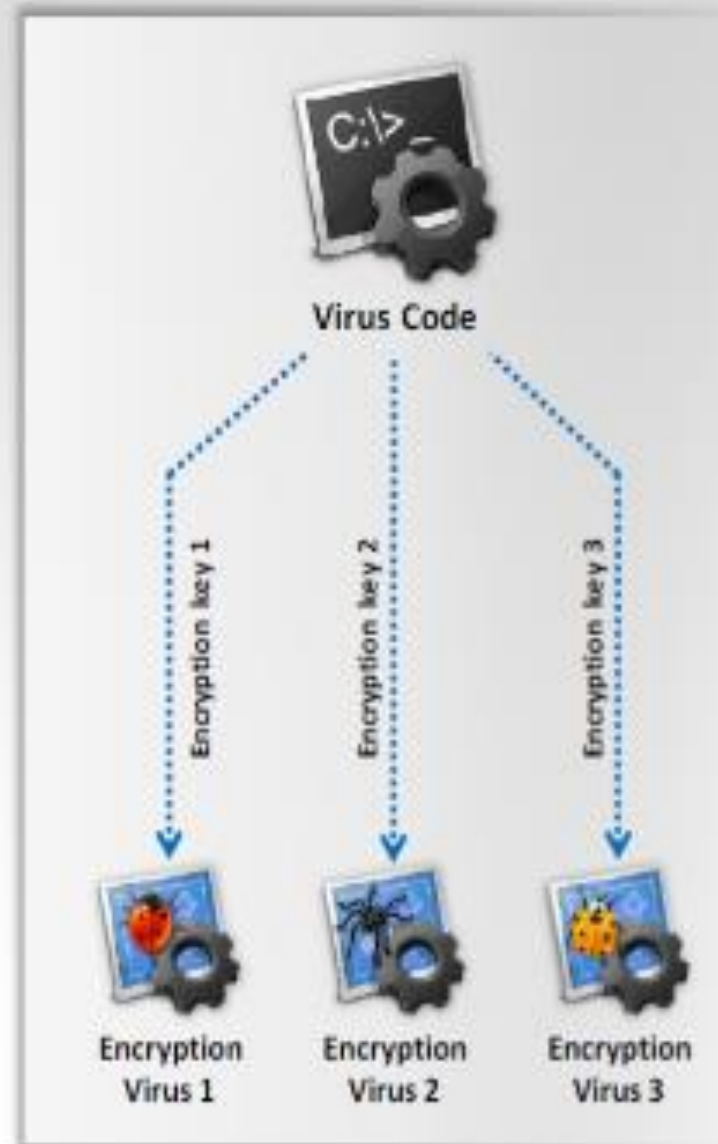
duyn@uit.edu.vn

This type of virus uses simple **encryption** to encipher the code



The virus is encrypted with a **different key** for each infected file

**AV scanner** cannot directly detect these types of viruses using signature detection methods





# Nội Dung

49

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- Cách phát hiện Trojan
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- Phân loại Virus
- **Worm máy tính**
- Cách phát hiện Virus

# Worm máy tính

50

duyn@uit.edu.vn

1

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction



Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system

2

3

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks



# Worm máy tính

## Sự khác biệt cơ bản giữa Virus và Worm

51

duyn@uit.edu.vn



*Replicates on its own*

A worm is a special type of virus that can replicate itself and **use memory**, but **cannot attach** itself to other programs

A worm takes advantage of **file** or **information** transport features on computer systems and spreads through the **infected network** automatically but a virus does not

*Spreads through the Infected Network*



# Nội Dung

52

duyn@uit.edu.vn

- Tổng quan về Trojan
- Quá trình lây nhiễm Trojan
- Phân loại Trojan
- Cách phát hiện Trojan
- Khái niệm Virus và Worm
- Quá trình lây nhiễm Virus
- Phân loại Virus
- Worm máy tính
- **Cách phát hiện Virus**



# Nội Dung

## Cách phát hiện Virus

53

duyn@uit.edu.vn



Question ???