

# Mã độc

## Chương 1. Tổng quan về mã độc

# Mục tiêu

- **Cung cấp một số kiến thức cơ bản về mã độc**
- **Giới thiệu cơ chế hoạt động của một số loại mã độc chính**

# Tài liệu tham khảo

**[1] TS. Lương Thế Dũng, KS. Hoàng Thanh Nam,  
2013, Giáo trình Mã độc, Học viện kỹ thuật Mật mã**

# Nội dung

**1. Mã độc**

**2. Phân loại mã độc**

**3. Cơ chế hoạt động của mã độc**

# Nội dung

**1. Mã độc**

**2. Phân loại mã độc**

**3. Cơ chế hoạt động của mã độc**

# Mã độc

- ☐ Định nghĩa mã độc
- ☐ Lịch sử của mã độc
- ☐ Mục đích của mã độc
- ☐ Con đường lây nhiễm mã độc

# Mã độc

- ☐ Định nghĩa mã độc
- ☐ Lịch sử của mã độc
- ☐ Mục đích của mã độc
- ☐ Con đường lây nhiễm mã độc

# Định nghĩa mã độc

- ❑ Mã độc (Malwares) là những chương trình máy tính độc hại với mục tiêu là đánh cắp thông tin, phá hủy hay làm hư hỏng hệ thống.
- ❑ Những chương trình này xâm nhập hệ thống một cách trái phép (không có sự cho phép của người quản trị).



# Định nghĩa mã độc

❑ Mã độc (Tên tiếng Anh là Malware hay Malicious software) là các chương trình máy tính được tạo ra với mục đích làm hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của dữ liệu, ứng dụng và hệ điều hành của của hệ thống.

# Mã độc

- ❑ Định nghĩa mã độc
- ❑ Lịch sử của mã độc
- ❑ Mục đích của mã độc
- ❑ Con đường lây nhiễm mã độc

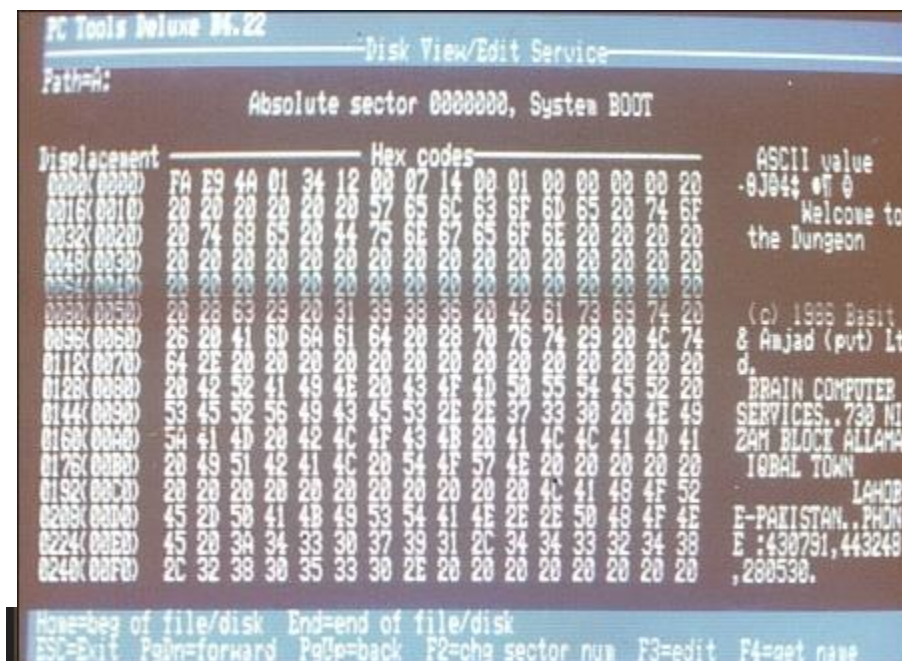
# Lịch sử của mã độc

- ❑ Lịch sử của mã độc có thể coi được bắt đầu từ năm 1949 khi lý thuyết đầu tiên về các chương trình tự sao chép ra đời.
- ❑ Năm 1981 loại mã độc đầu tiên gọi là virus mới xuất hiện, virus này có tên là **Apple II**.

# Lịch sử của mã độc

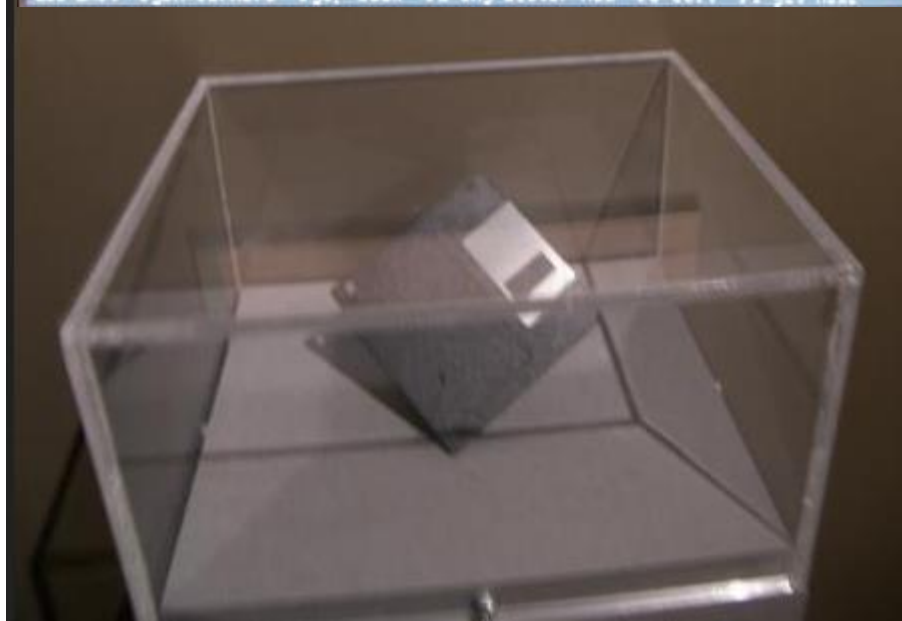
❑ Năm 1986 virus Brain âm thầm đổ bộ từ Pakistan vào nước Mỹ với mục tiêu đầu tiên là Trường Đại học Delaware.

❑ 2/11/1988: Robert Morris đưa virus vào mạng máy tính quan trọng nhất của Mỹ, gây thiệt hại lớn. .



The screenshot shows a DOS disk view of a boot sector infected with the Brain virus. The title bar reads "PC Tools Deluxe B1.22" and "Disk View/Edit Service". The path is "A:". The absolute sector is 0000000, System BOOT. The display is divided into three columns: Displacement, Hex codes, and ASCII value. The hex codes show the virus signature "FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20" at offset 0000. The ASCII value column shows "Welcome to the Dungeon" and copyright information for Basit & Amjad (pvt) Lt d. The footer contains navigation instructions: Home=begin of file/disk, End=end of file/disk, ESC=Exit, PgDn=forward, PgUp=back, F2=chg sector num, F3=edit, F4=get name.

Displacement	Hex codes	ASCII value
0000(0000)	FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20	-9J04; 07 0
0016(0010)	20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F	Welcome to
0032(0020)	20 74 6F 65 20 44 75 6E 67 65 6F 6E 20 20 20 20	the Dungeon
0048(0030)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0064(0040)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080(0050)	20 20 63 23 20 31 33 38 36 20 42 61 73 65 74 20	(c) 1988 Basit
0096(0060)	26 20 41 60 6A 61 64 20 20 70 76 74 29 20 4C 74	& Amjad (pvt) Lt
0112(0070)	64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20	d.
0128(0080)	20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20	BRAIN COMPUTER
0144(0090)	53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49	SERVICES..730 NI
0160(00A0)	54 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41	2AM BLOCK ALLAMA
0176(00B0)	20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20	IOBAL TOWN
0192(00C0)	20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52	LAHOR
0208(00D0)	45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E	E-PAKISTAN..PHON
0224(00E0)	45 2D 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38	E :430791,443248
0240(00F0)	2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20	,280530.

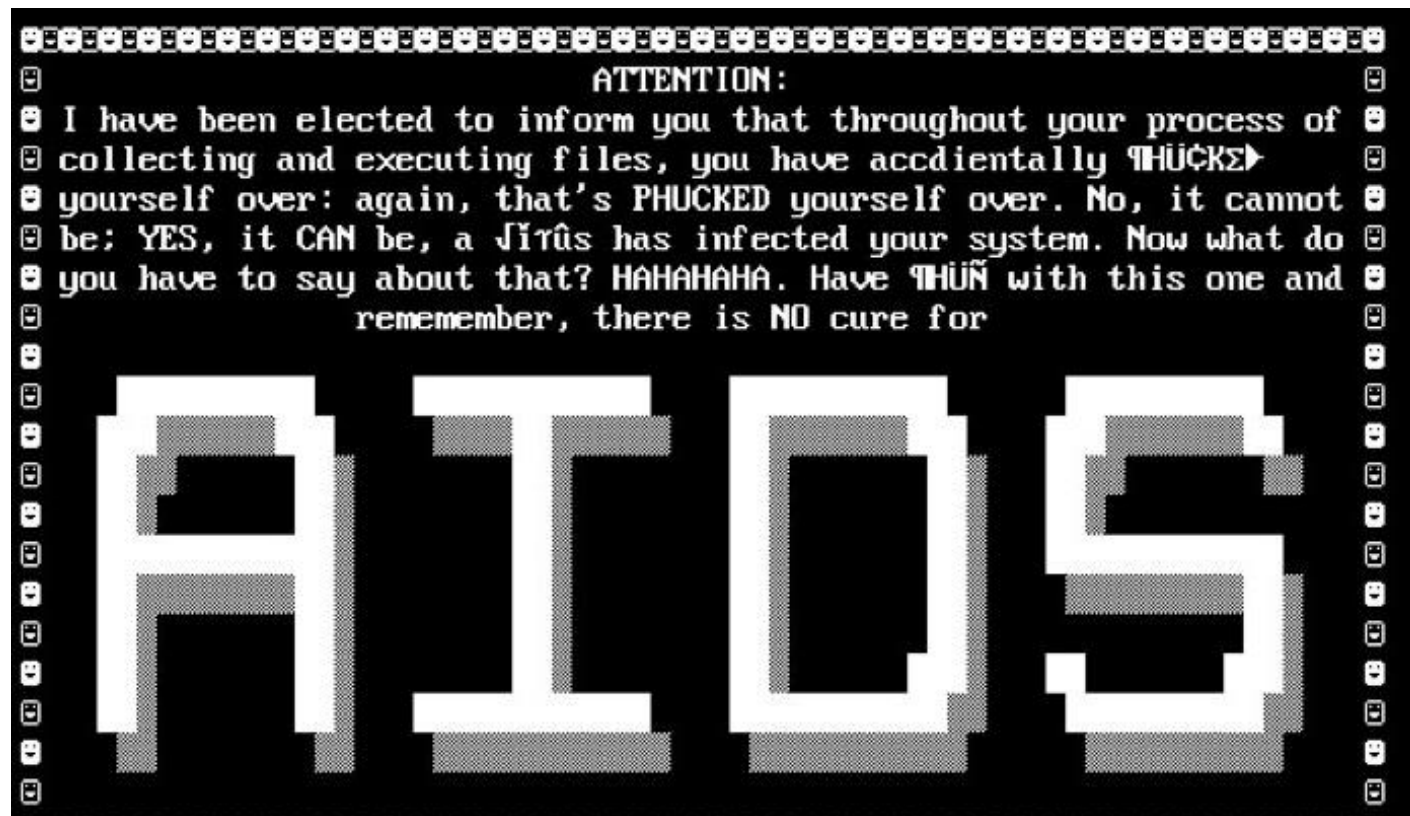


# Lịch sử của mã độc

❑ Năm 1988: Virus Jerusalem xuất hiện, được kích hoạt vào thứ sáu ngày 13.

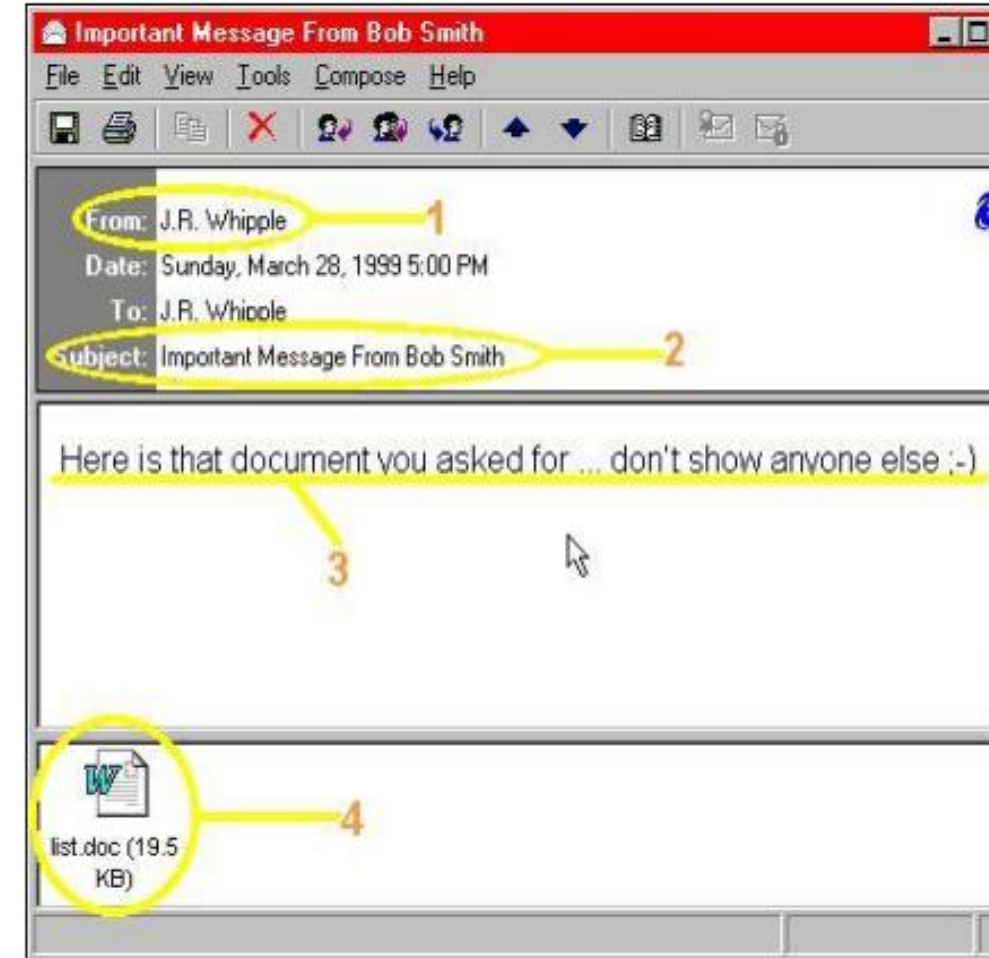
❑ Năm 1989: Xuất hiện chương trình Trojan có tên

AIDS.



# Lịch sử của mã độc

- ❑ Năm 1991: Tequila, một trong những virus phát tán dưới nhiều hình dạng đầu tiên được phát hiện.
- ❑ Năm 1996: Virus macro và virus Staog xuất hiện lần đầu tiên.
- ❑ Năm 1996: Virus Boza. Virus đầu tiên trên hệ điều hành Windows95.



# Lịch sử của mã độc

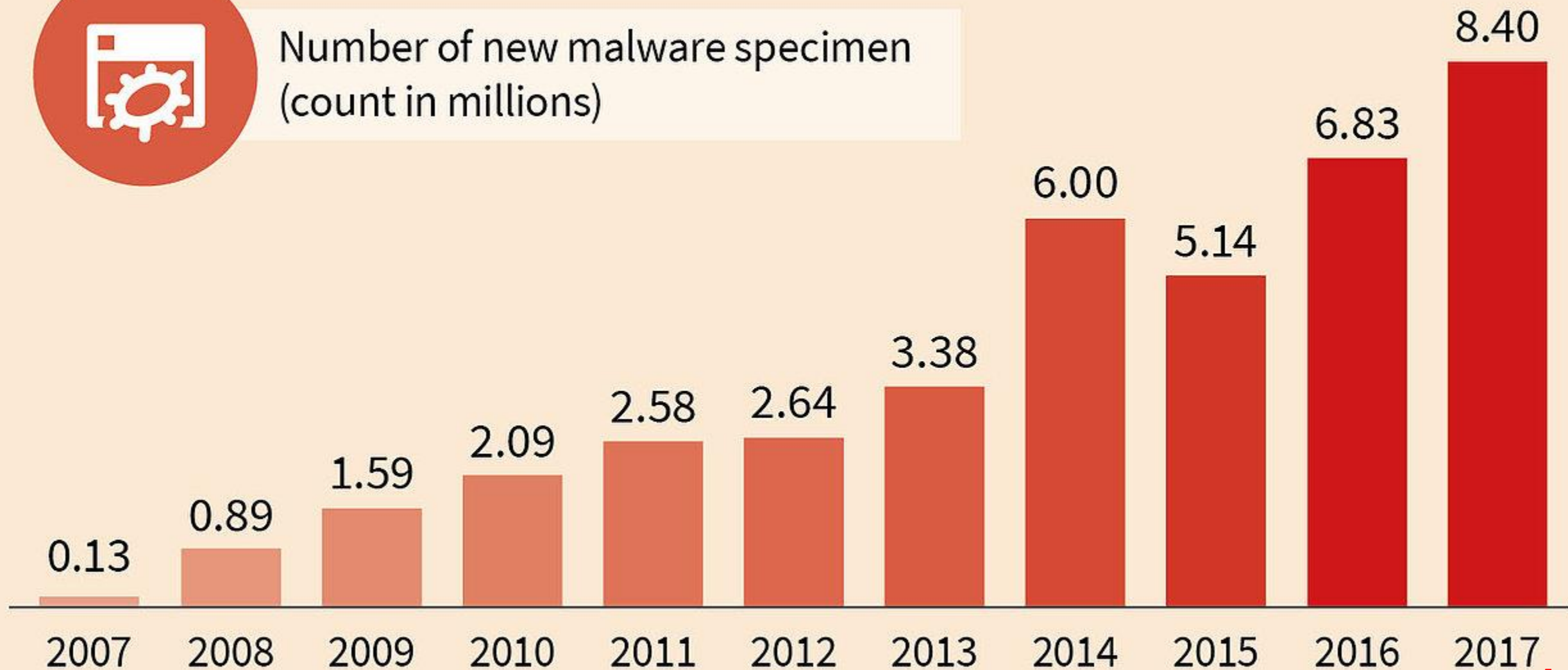
- ❑ Năm 1998: Strange Brew là virus đầu tiên lây nhiễm vào file Java.
- ❑ Năm 2001: Virus Winux (Windows/Linux), Nimda, Code Red. Virus Winux đánh dấu dòng virus có thể lây được trên các hệ điều hành Linux chứ không chỉ Windows.



# Lịch sử của mã độc

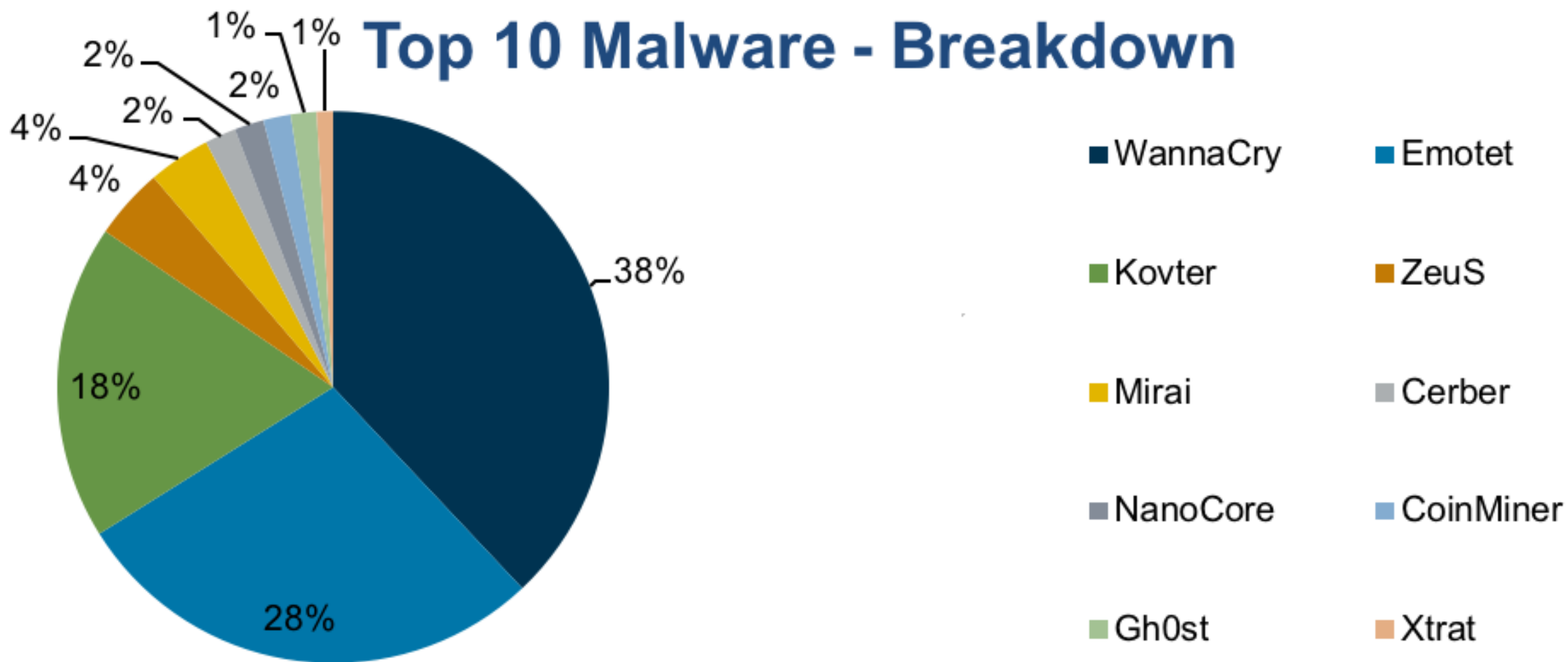


Number of new malware specimen  
(count in millions)





# Lịch sử của mã độc





# Mã độc

- ❑ Định nghĩa mã độc
- ❑ Lịch sử của mã độc
- ❑ Mục đích của mã độc
- ❑ Con đường lây nhiễm mã độc

# Mục đích của mã độc

- ☐ **Hiển thị các quảng cáo;**
- ☐ **Gian lận, lừa đảo;**
- ☐ **Theo dõi hoạt động, lấy cắp thông tin của người dùng;**
- ☐ **Chiếm quyền điều khiển máy tính;**
- ☐ **Phá hoại hệ thống...**

# Mã độc

- ❑ Định nghĩa mã độc
- ❑ Lịch sử của mã độc
- ❑ Mục đích của mã độc
- ❑ Con đường lây nhiễm mã độc

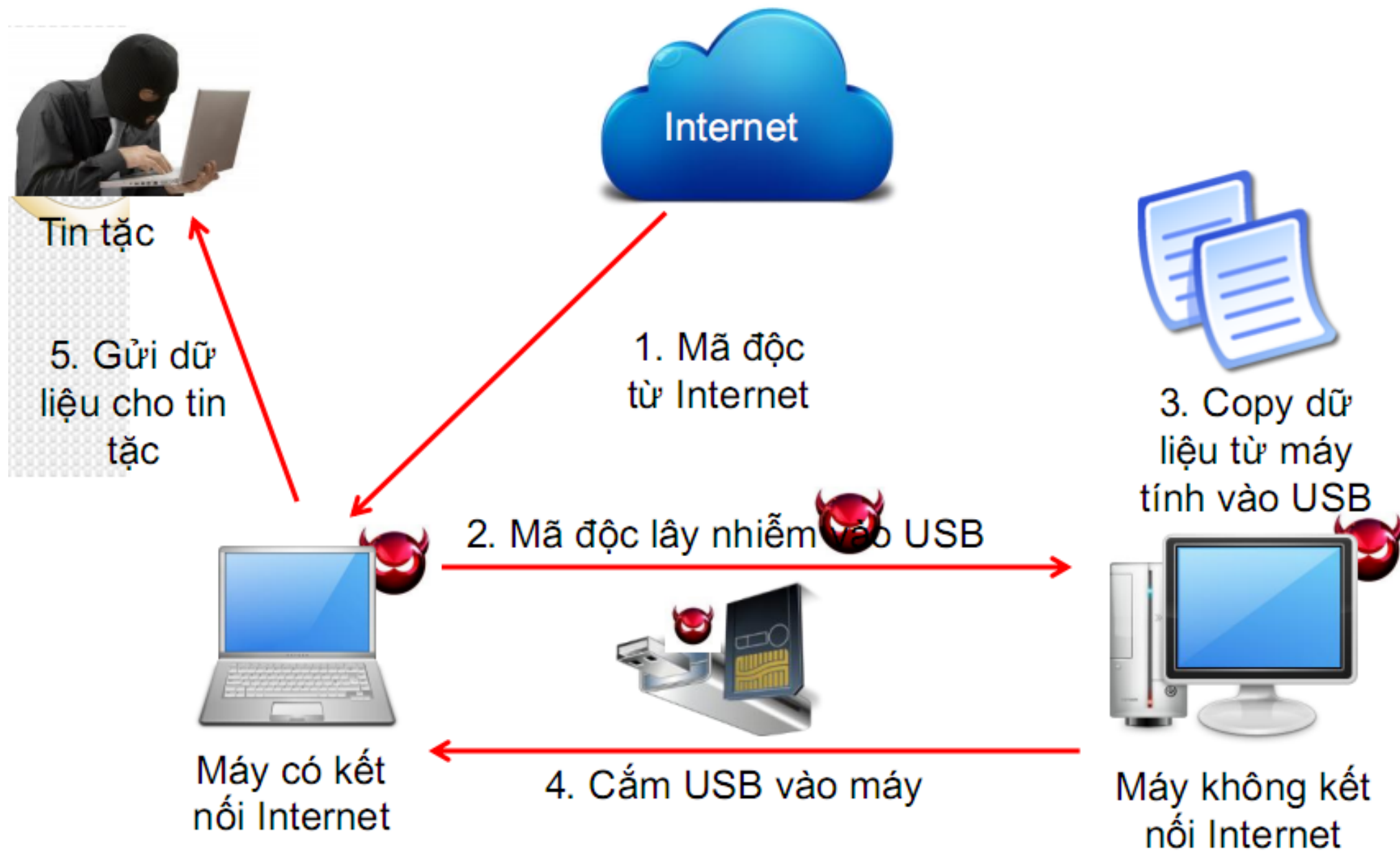
# Con đường lây nhiễm mã độc

- ☐ Qua các thiết bị lưu trữ di động
- ☐ Qua thư điện tử
- ☐ Qua trình duyệt web
- ☐ Lây nhiễm từ smartphone sang máy tính

# Con đường lây nhiễm mã độc

- ❑ Qua các thiết bị lưu trữ di động
- ❑ Qua thư điện tử
- ❑ Quá trình duyệt web
- ❑ Lây nhiễm từ smartphone sang máy tính

# Qua các thiết bị lưu trữ di động





# Qua các thiết bị lưu trữ di động

❑ Hình thức lây nhiễm: Mã độc lây nhiễm từ máy có kết nối Internet sang máy không kết nối Internet hoặc lây nhiễm từ máy tính này sang máy tính khác thông qua USB.

❑ Cơ chế lây nhiễm:

- Khi cắm USB vào máy kết nối Internet, mã độc lây nhiễm vào USB (bằng các đường lây nhiễm kể trên).
- Cắm USB sang máy không kết nối Internet, mã độc lây nhiễm vào máy này.

# Qua các thiết bị lưu trữ di động

❑ Cơ chế lấy cắp dữ liệu: Mã độc tự động copy dữ liệu từ máy không nối Internet vào USB ở dạng ẩn.

- Khi cắm USB sang máy có nối Internet, mã độc gửi tài liệu từ

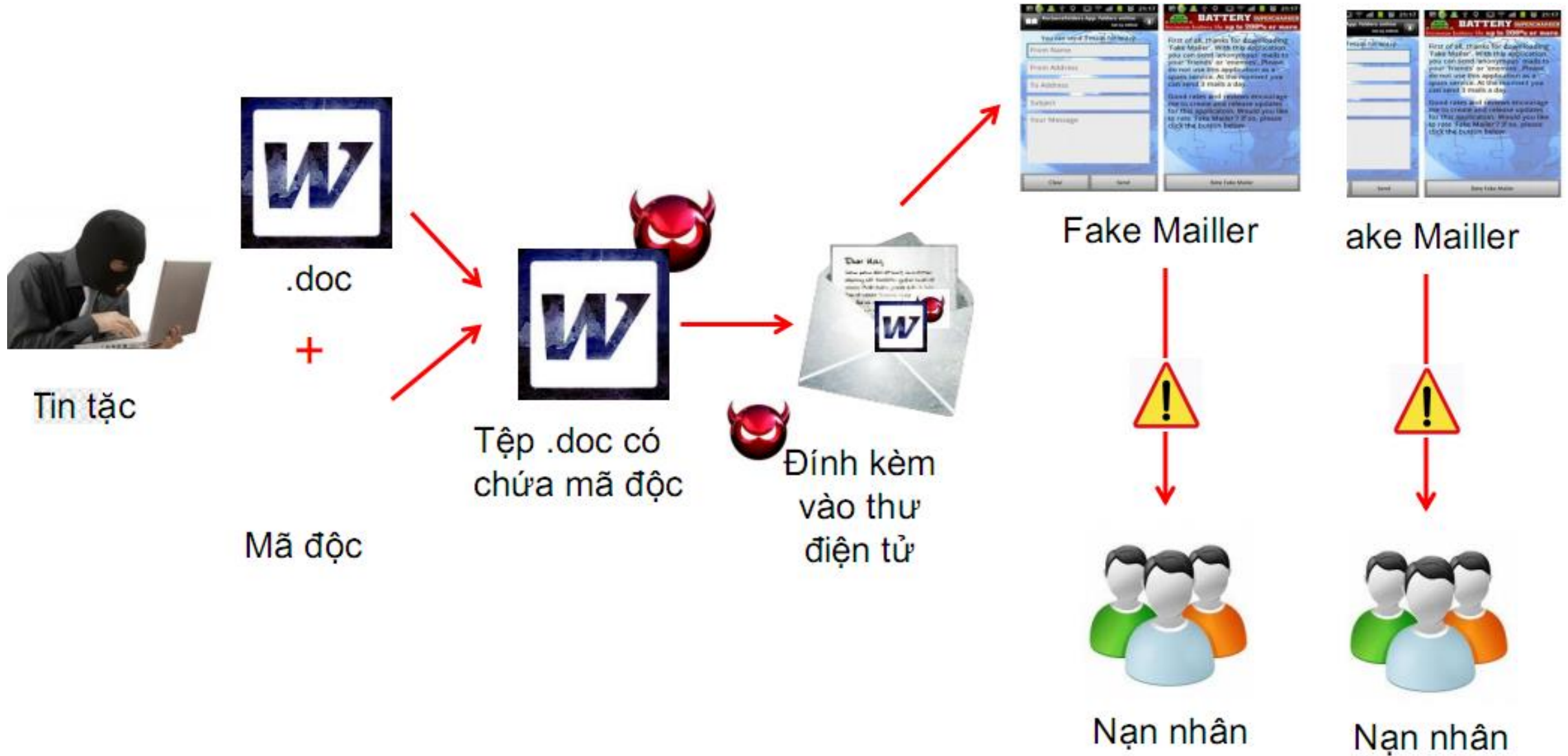
- USB đến hòm thư hoặc máy tính đích của tin tặc.

Ví dụ: **W32.XFileUSB**

# Con đường lây nhiễm mã độc

- ❑ Qua các thiết bị lưu trữ di động
- ❑ Qua thư điện tử
- ❑ Quá trình duyệt web
- ❑ Lây nhiễm từ smartphone sang máy tính

# Qua thư điện tử



# Qua thư điện tử

Ngày Thứ 4, 25/07/12, NguyenThi LanHuong <lhuor[redacted]m> đã viết:

Từ: NguyenThi LanHuong <lhuor[redacted]com>

Chủ đề: Danh sach tang luong Cui Nam 2012



Đến: duor[redacted]com

Ngày: Thứ Tư, 25 tháng 7, 2012, 11:09

Chu y Danh sach co loi ko? .

 **DanhSachTangLuong.xls**  
77K View Open as a Google spreadsheet Download

From: Nguyễn [redacted] <nt[redacted]hcn@bac[redacted].vn>  
Date: 2013/2/5  
Subject: Công văn gửi đến cơ quan HCM  
To: [redacted]

 Công văn cung cấp địa chỉ mail.7z (375 KB)  
 Lưu tất cả các files

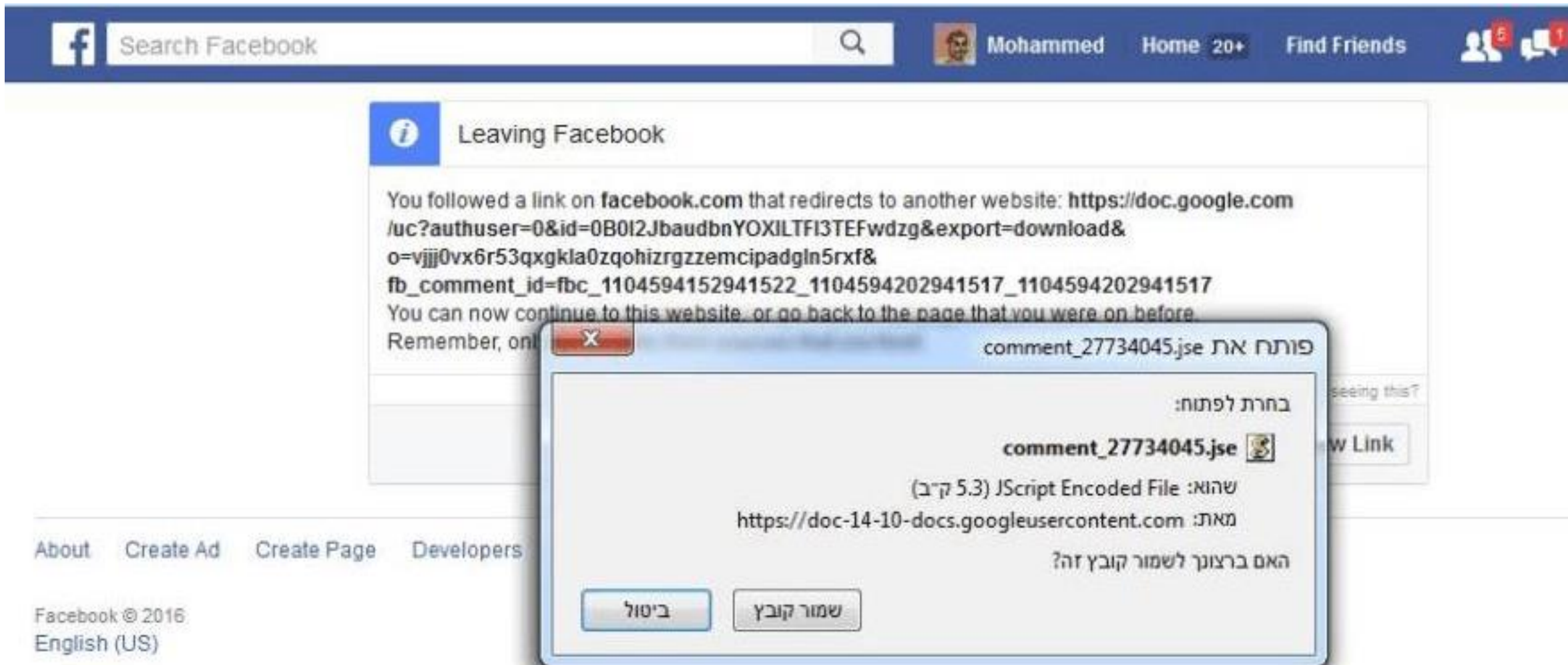
Tôi xin kính gửi công văn mới nhất từ Sở Thông Tin Truyền Thông TP.HCM và đề nghị anh (chị) ở các cơ quan truyền thông xem qua rồi phổ biến cho các đồng nghiệp khác cùng cơ quan-sở.  
Cảm ơn anh (chị).

--  
Nguyễn [redacted] - Tổng biên tập Tạp chí [redacted]

# Con đường lây nhiễm mã độc

- ❑ Qua các thiết bị lưu trữ di động
- ❑ Qua thư điện tử
- ❑ **Quá trình duyệt web**
- ❑ Lây nhiễm từ smartphone sang máy tính

# Quá trình duyệt web



# Con đường lây nhiễm mã độc

- ❑ Qua các thiết bị lưu trữ di động
- ❑ Qua thư điện tử
- ❑ Quá trình duyệt web
- ❑ Lây nhiễm từ smartphone sang máy tính



# Lây nhiễm từ smartphone sang máy tính



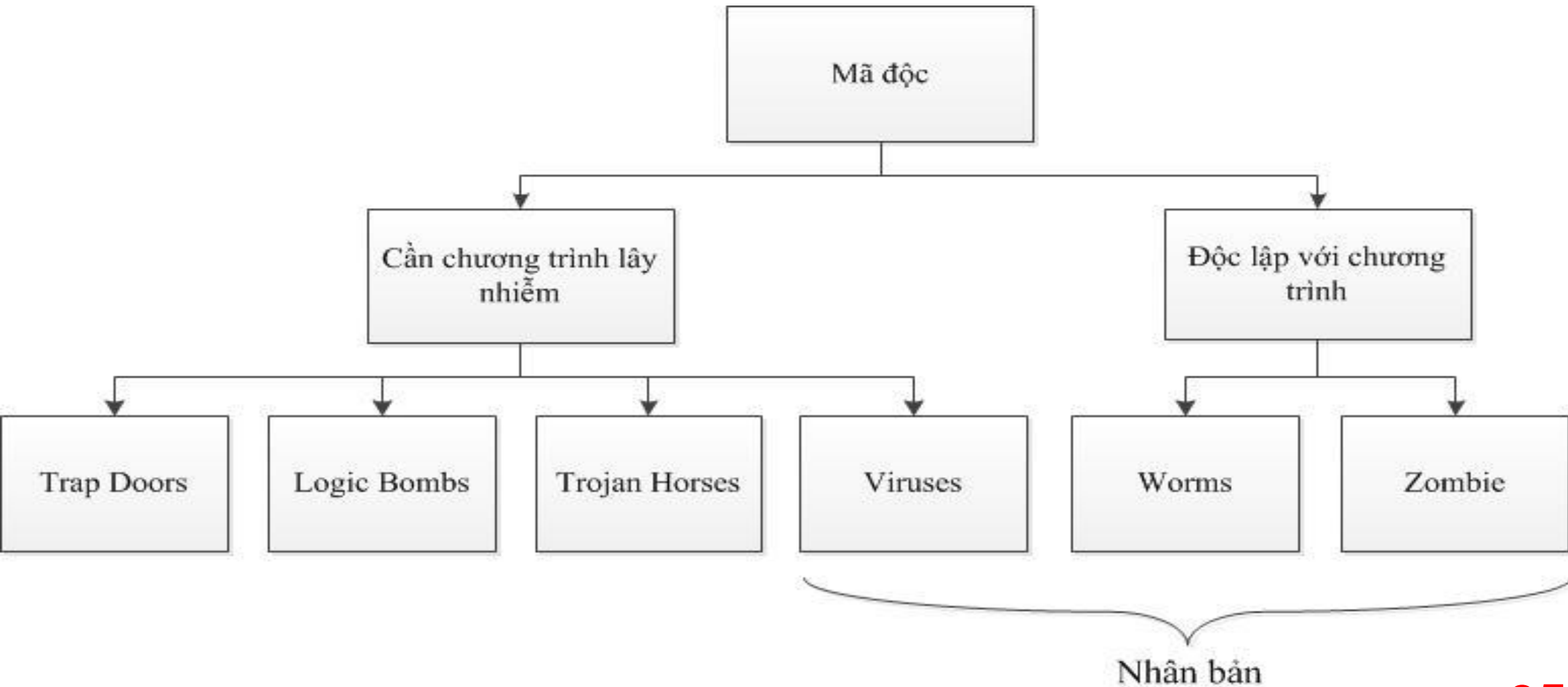
# Nội dung

**1. Mã độc**

**2. Phân loại mã độc**

**3. Cơ chế hoạt động của mã độc**

# Phân loại mã độc



# Nội dung

**1. Mã độc**

**2. Phân loại mã độc**

**3. Cơ chế hoạt động của mã độc**

# Cơ chế hoạt động của mã độc

- ☐ Virus
- ☐ Worm
- ☐ Trojan horse



# Cơ chế hoạt động của mã độc

☐ **Virus**

☐ **Worm**

☐ **Trojan horse**

# Virus

**❑ Là một loại mã độc có khả năng tự nhân bản và lây nhiễm chính nó vào các tệp, chương trình máy tính.**

# Virus

Vòng đời virus gồm 4 giai đoạn:

- ❑ Trú ẩn (Dormant)
- ❑ Lây lan (Propagation)
- ❑ Kích hoạt (Triggering)
- ❑ Thực thi (Execution)





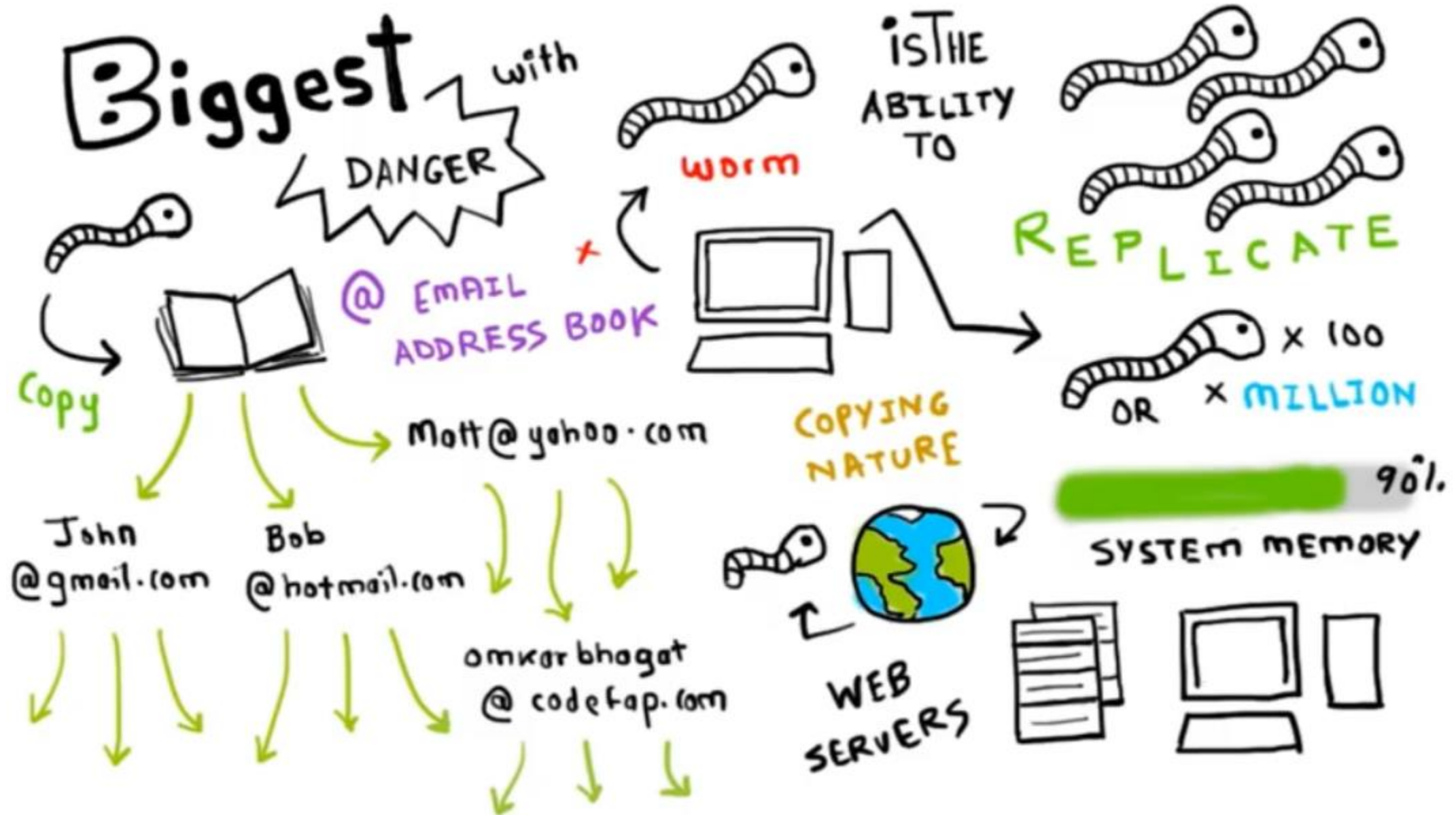
# Cơ chế hoạt động của mã độc

☐ Virus

☐ Worm

☐ Trojan horse

# Worm



# Worm

- ❑ Worm là chương trình độc hại có khả năng tự nhân bản và tự lây nhiễm trong hệ thống mà không cần tệp chủ để mang nó.
- ❑ Làm lãng phí băng thông của mạng, phá hoại hệ thống như xóa tệp, tạo ra cửa sau cho phép tin tặc kiểm soát máy tính của nạn nhân

# Worm

**Cơ chế hoạt động:**

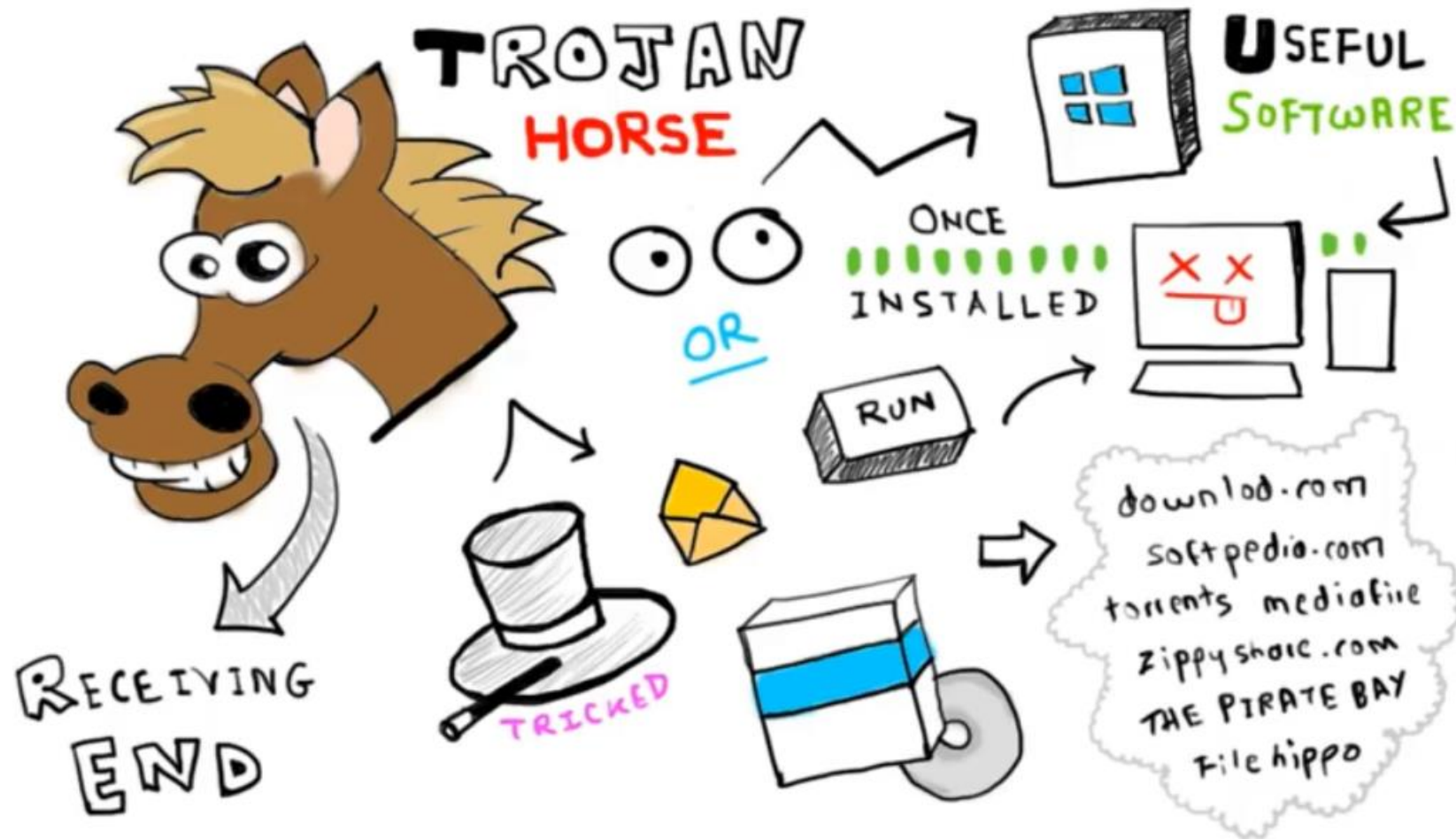
- ☐ **Tìm kiếm các đối tượng phù hợp,**
- ☐ **Lây nhiễm,**
- ☐ **Tự sao chép bản thân nó vào các thư mục hệ thống đồng thời ghi thông tin khởi động vào hệ thống.**

# Cơ chế hoạt động của mã độc

- ☐ Virus
- ☐ Worm
- ☐ Trojan horse

# Trojan Horse

- ❑ Không có khả năng tự nhân bản
- ❑ Bên trong có ẩn chứa các đoạn mã với mục đích gây hại

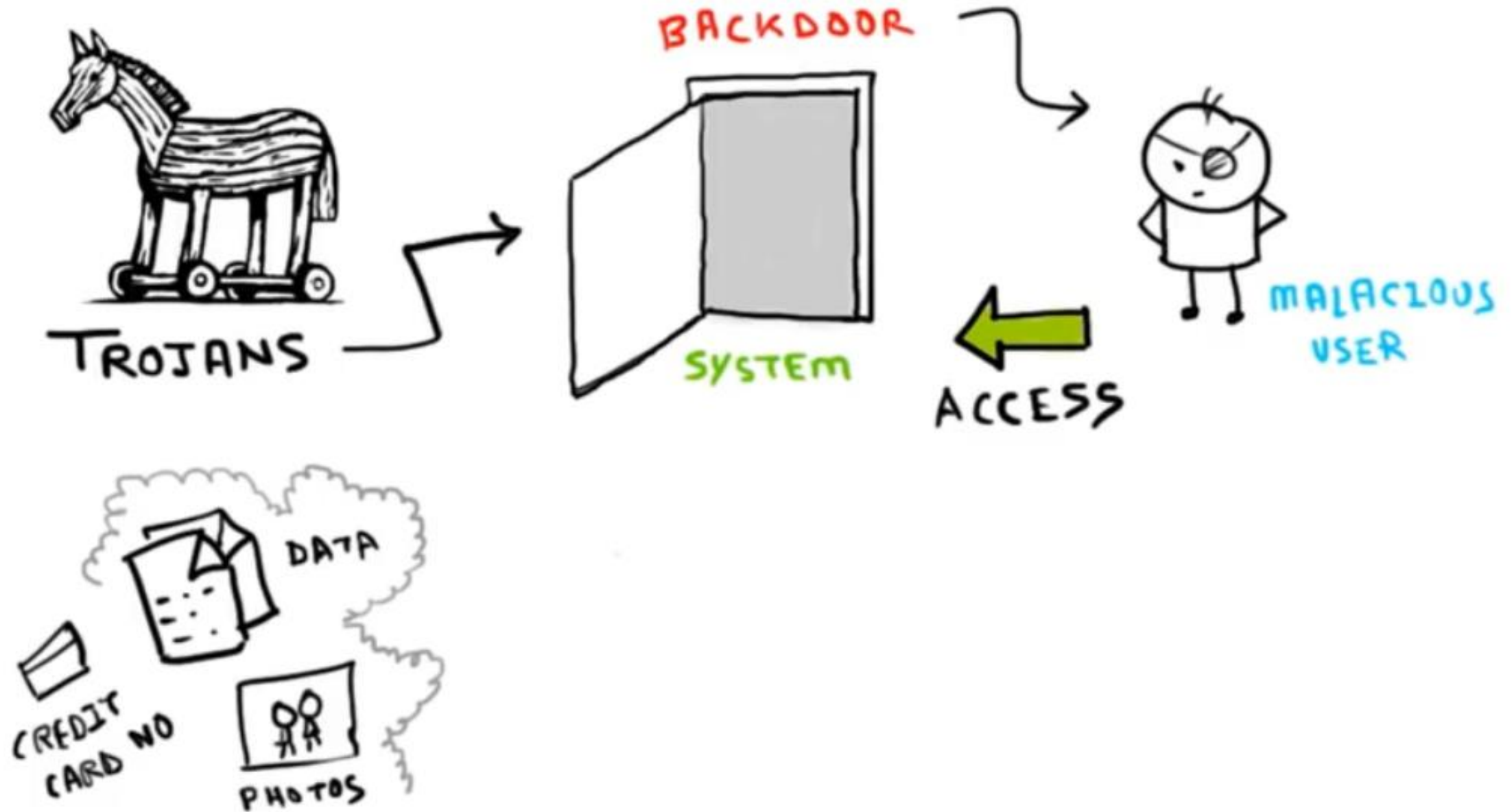


# Trojan Horse

**Trojan có thể gây hại theo ba cách sau:**

- ❑ Thực hiện các chức năng của chương trình chủ bình thường, đồng thời thực thi các hoạt động gây hại một cách riêng biệt**
- ❑ Thực thi các chức năng của chương trình chủ, nhưng sửa đổi một số chức năng để gây tổn hại hoặc che giấu các hành động phá hoại khác**
- ❑ Thực thi luôn một chương trình gây hại bằng cách núp dưới danh một chương trình không có hại**

# Trojan Horse





# Trojan Horse

**Các loại Trojan điển hình:**

- ☐ Trojan truy cập từ xa
- ☐ Trojan gửi dữ liệu
- ☐ Trojan phá hoại
- ☐ Trojan tắt phần mềm an ninh
- ☐ Trojan DoS

# Nội dung

**1. Mã độc**

**2. Phân loại mã độc**

**3. Cơ chế hoạt động của mã độc**