CƠ SỞ AN TOÀN THÔNG TIN

Bài 7. Phòng chống mã độc

1. Khái niệm mã độc
2. Con đường lây nhiễm mã độc
3. Phòng chống mã độc

1 Khái niệm mã độc

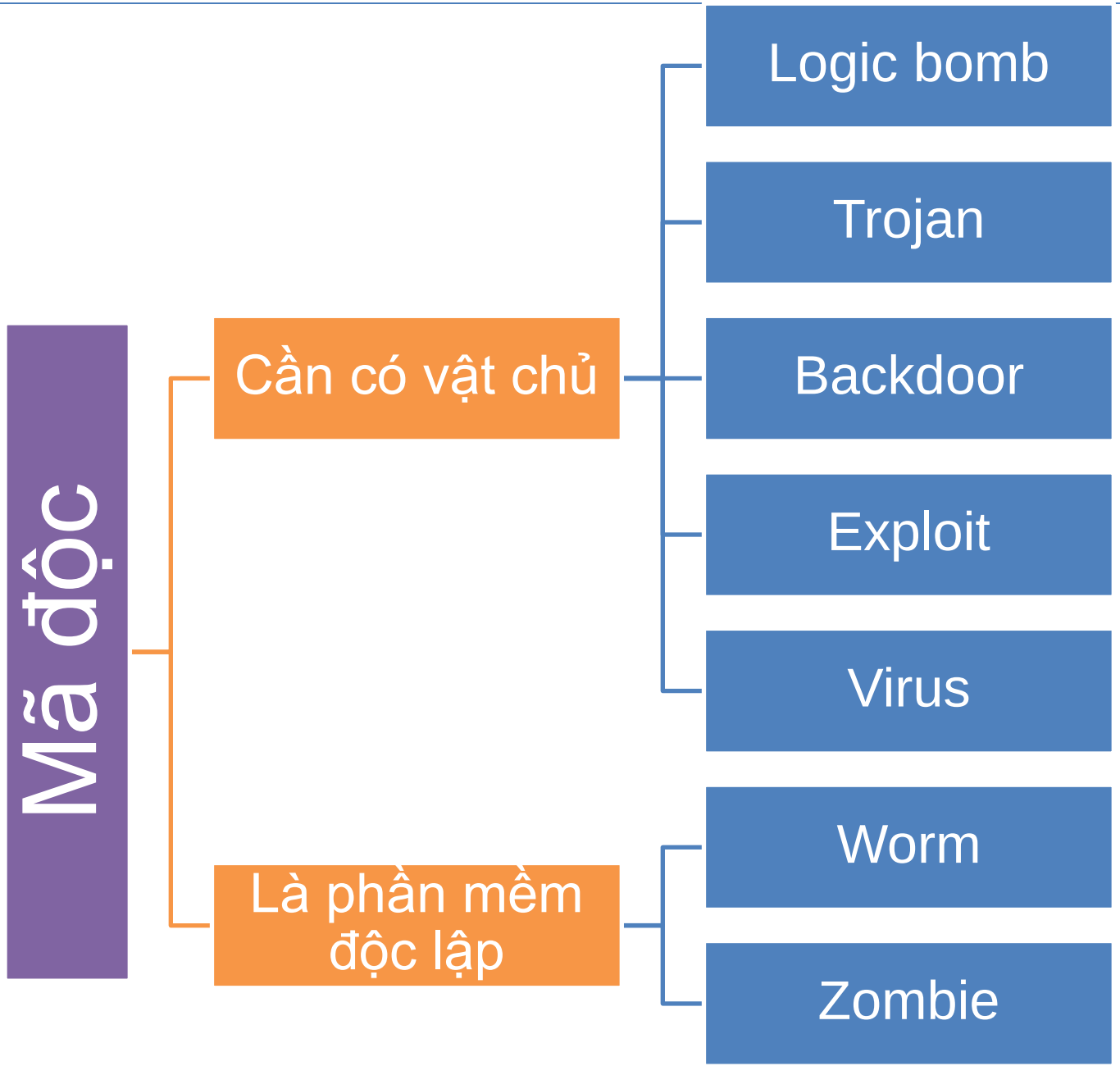
2 Con đường lây nhiễm mã độc

3 Phòng chống mã độc

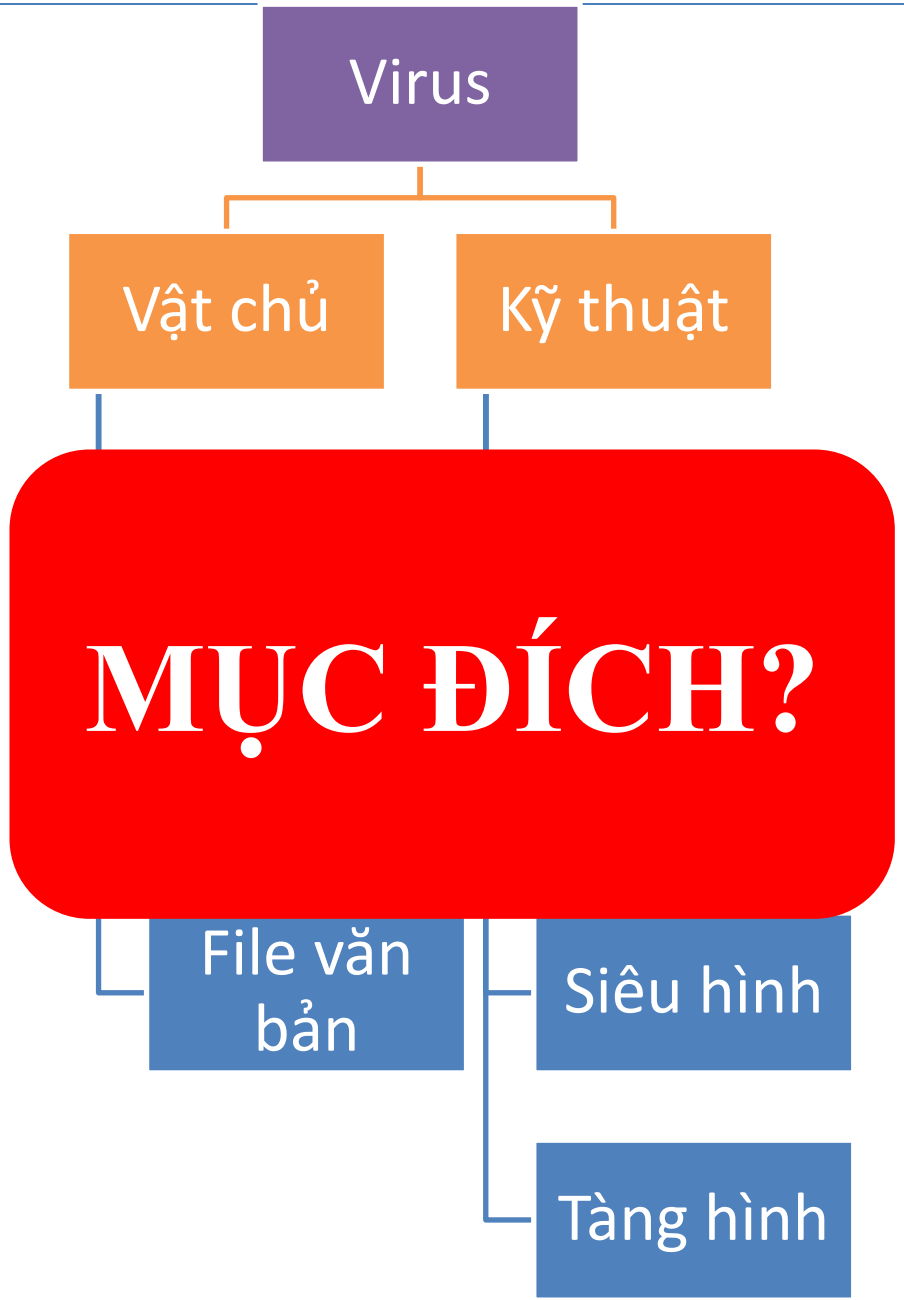
Khái niệm mã độc

- **Mã độc (Malware)** là những 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 (malware)** là những chương trình máy tính được tạo ra với mục đích xấu!

Phân loại mã độc



Phân loại mã độc



Mục đích của mã độc (1/2)

- Thu thập dữ liệu trên máy tính
- Ăn cắp thông tin như mật khẩu, mã bảo mật thẻ tín dụng.
- Nghe lén thông tin như chụp màn hình, ghi âm, quay màn hình, keylogger.
- Sử dụng máy tính của nạn nhân để tạo một mạng botnet phục vụ cho các tấn công DDOS.

Mục đích của mã độc (2/2)

- Sử dụng máy tính của nạn nhân để phát tán thư rác.
- Sử dụng tài nguyên trên máy nạn nhân (để "đào" Bitcoin).
- Mã hóa dữ liệu và đòi tiền chuộc.
- Phá hủy dữ liệu trên máy nạn nhân.
- Làm hư hại thiết bị phần cứng (Chernobyl, Stuxnet)
- ....

1 Khái niệm mã độc

2 Con đường lây nhiễm mã độc

3 Phòng chống mã độc

Các con đường lây nhiễm mã độc (1/9)

Qua thư điện tử

Qua USB

Sử dụng phần mềm lậu, phần mềm bẻ khóa

Từ website

Qua dịch vụ hội thoại trực tuyến (Chat)

Qua mạng xã hội

Qua mạng nội bộ

Cài đặt trực tiếp

Các con đường lây nhiễm mã độc (2/9)

❑Cài đặt trực tiếp

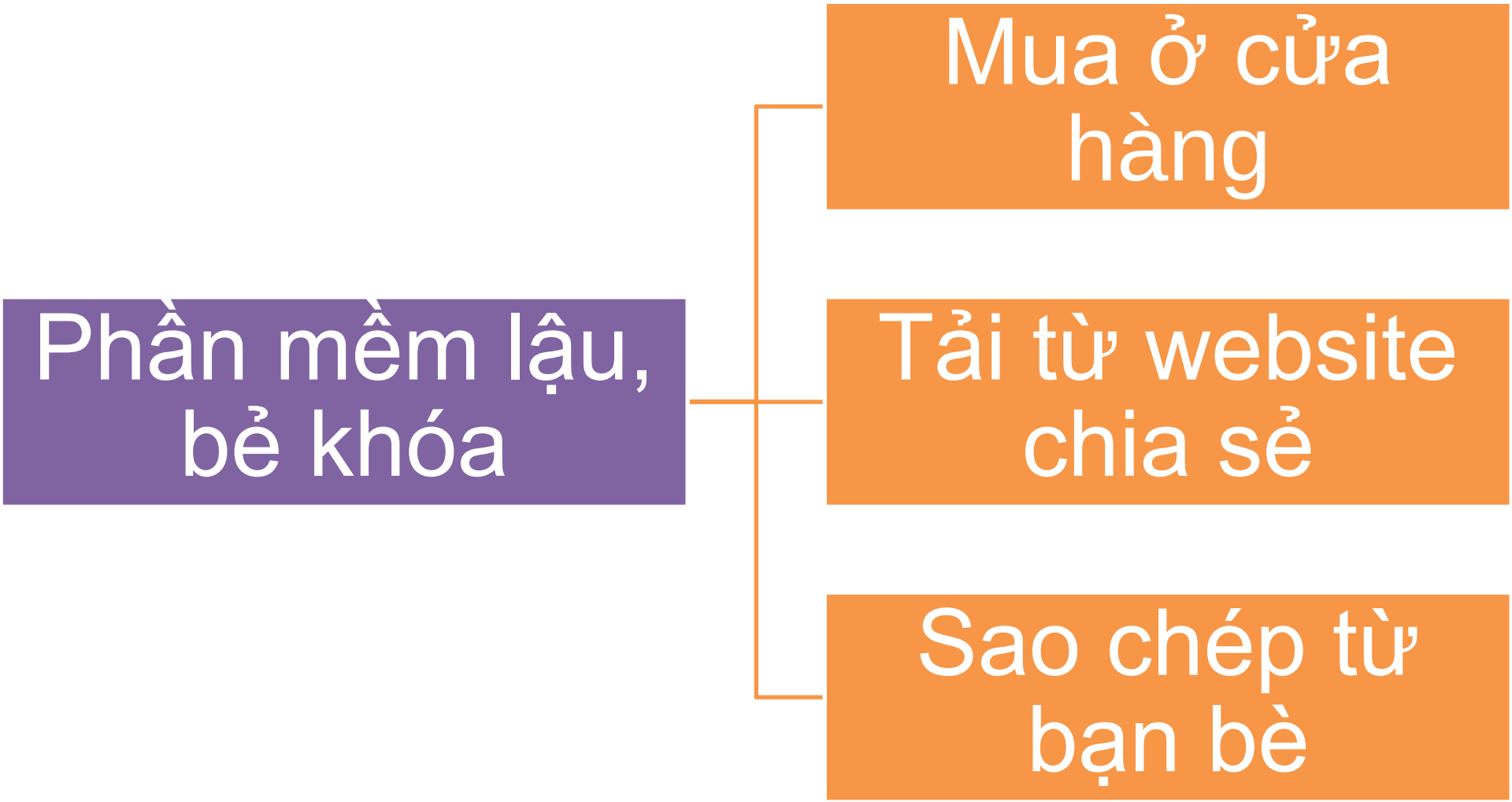
- Cho người khác mượn máy tính, smartphone
- Rời khỏi máy tính, smartphone mà không khóa hệ thống
- Máy bị nhiễm mã độc từ từ nhà sản xuất!

Các con đường lây nhiễm mã độc (3/9)

❑Phần mềm lậu, bẻ khóa

- Người bẻ khóa thường là thành viên của những nhóm cracker, hacker
- Phần mềm bẻ khóa thường bị nhúng mã độc để phục vụ mục đích của tin tặc
- Khi sử dụng những phần mềm như thế, mã độc sẽ phát tán vào máy và lây lan

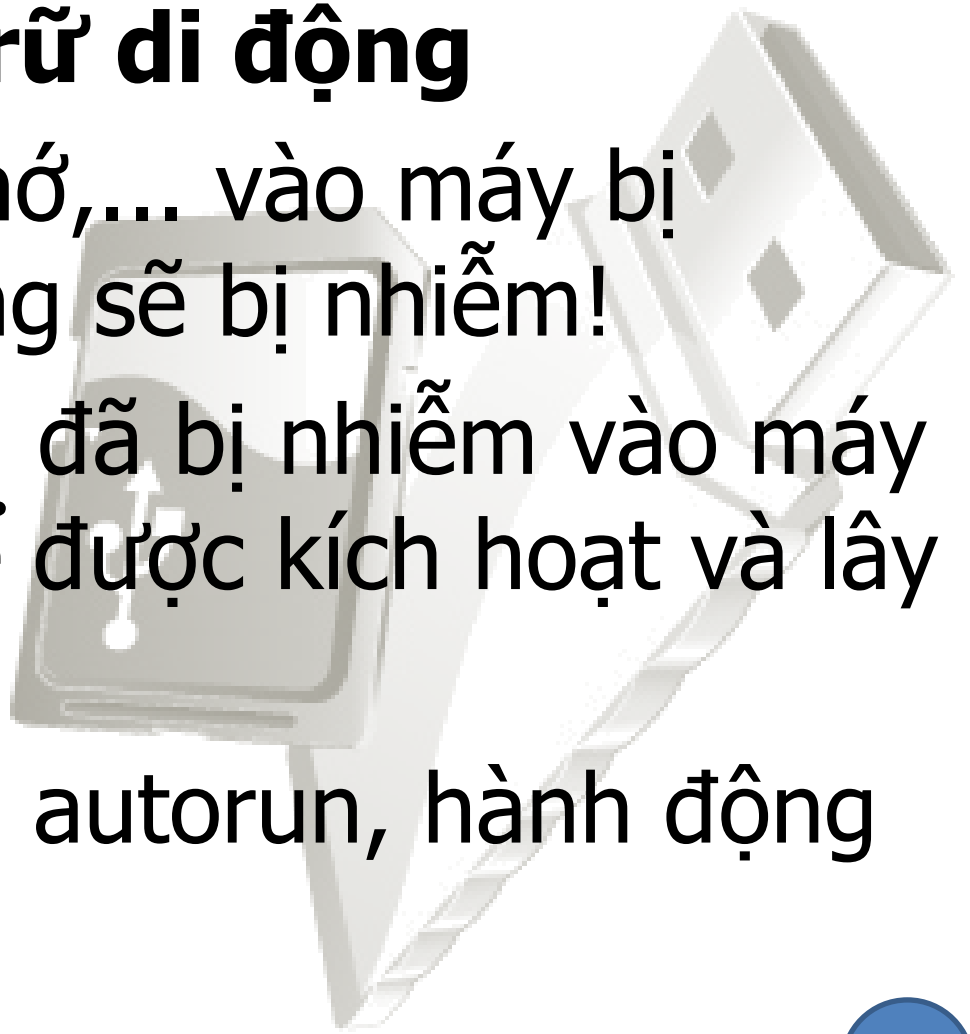
Các con đường lây nhiễm mã độc (4/9)



Các con đường lây nhiễm mã độc (5/9)

❑Qua thiết bị lưu trữ di động

- Khi cắm USB, thẻ nhớ,... vào máy bị nhiễm mã độc, chúng sẽ bị nhiễm!
- Cắm USB, thẻ nhớ... đã bị nhiễm vào máy khác, mã độc có thể được kích hoạt và lây nhiễm vào máy đó.
- Kích hoạt: tính năng autorun, hành động của người dùng

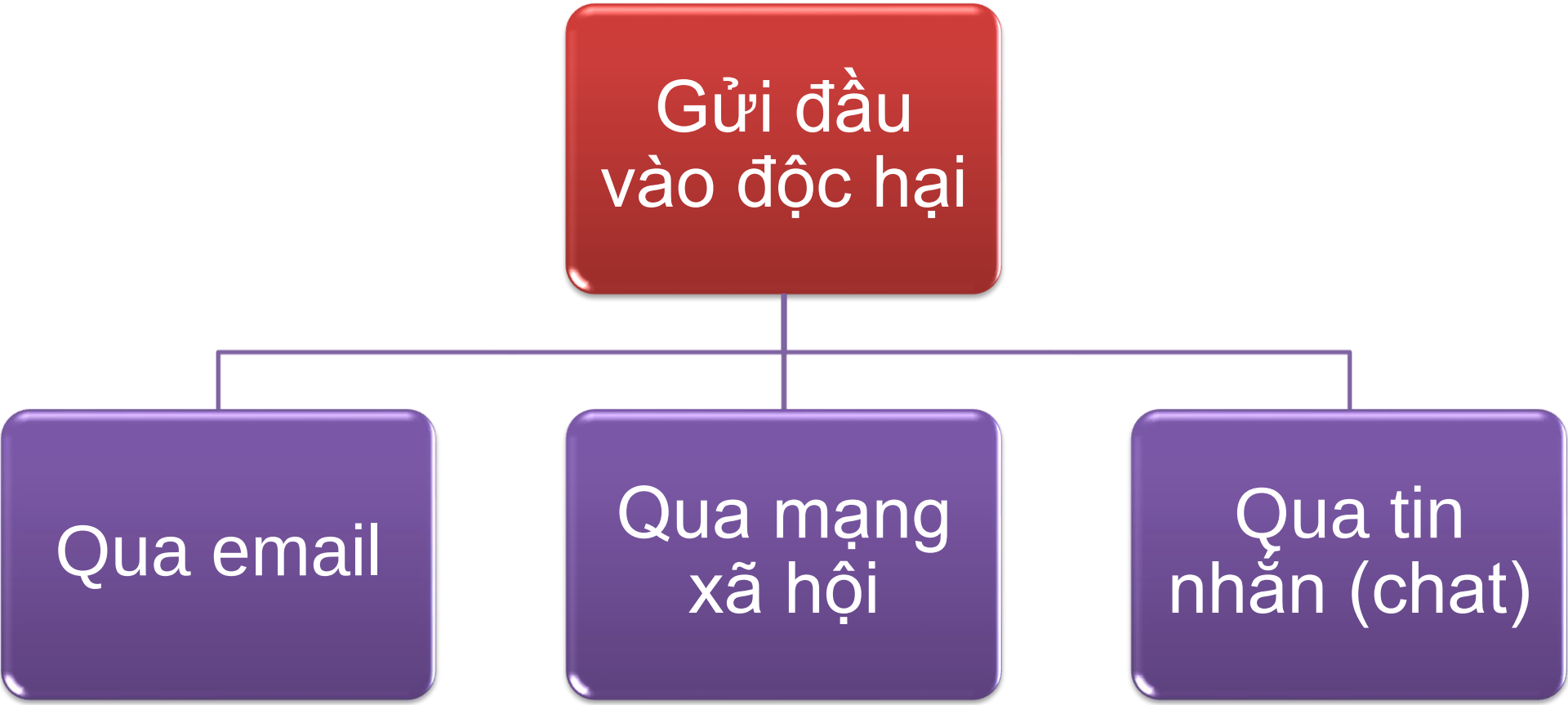


Các con đường lây nhiễm mã độc (6/9)

❑Khai thác lỗi phần mềm

- Phần mềm: hệ điều hành, phần mềm văn phòng, trình duyệt web, phần mềm chơi nhạc và video, game...
- Nhiều phần mềm có lỗi!
- Hacker tạo những đầu vào đặc biệt cho phần mềm (văn bản, trang web, file nhạc, gói tin...) trong đó có mã độc
- Khi phần mềm xử lý đầu vào đặc biệt đó thì mã độc được thực thi.

Các con đường lây nhiễm mã độc (7/9)



Hậu quả do mã độc

- Hiệu suất làm việc của máy bị giảm
- Khiến máy người khác cũng bị lây nhiễm (qua mạng LAN, qua USB, qua email...)
- Dữ liệu bị đánh cắp, bị khóa hoặc bị hủy
- Nếu mã độc là "bot" thì băng thông bị chiếm, IP của công ty (tổ chức) sẽ bị tường lửa chặn
- Nếu mã độc phát tán thư rác thì nhiều người bị ảnh hưởng.

Mã độc APT !?!?!?

1 Khái niệm mã độc

2 Con đường lây nhiễm mã độc

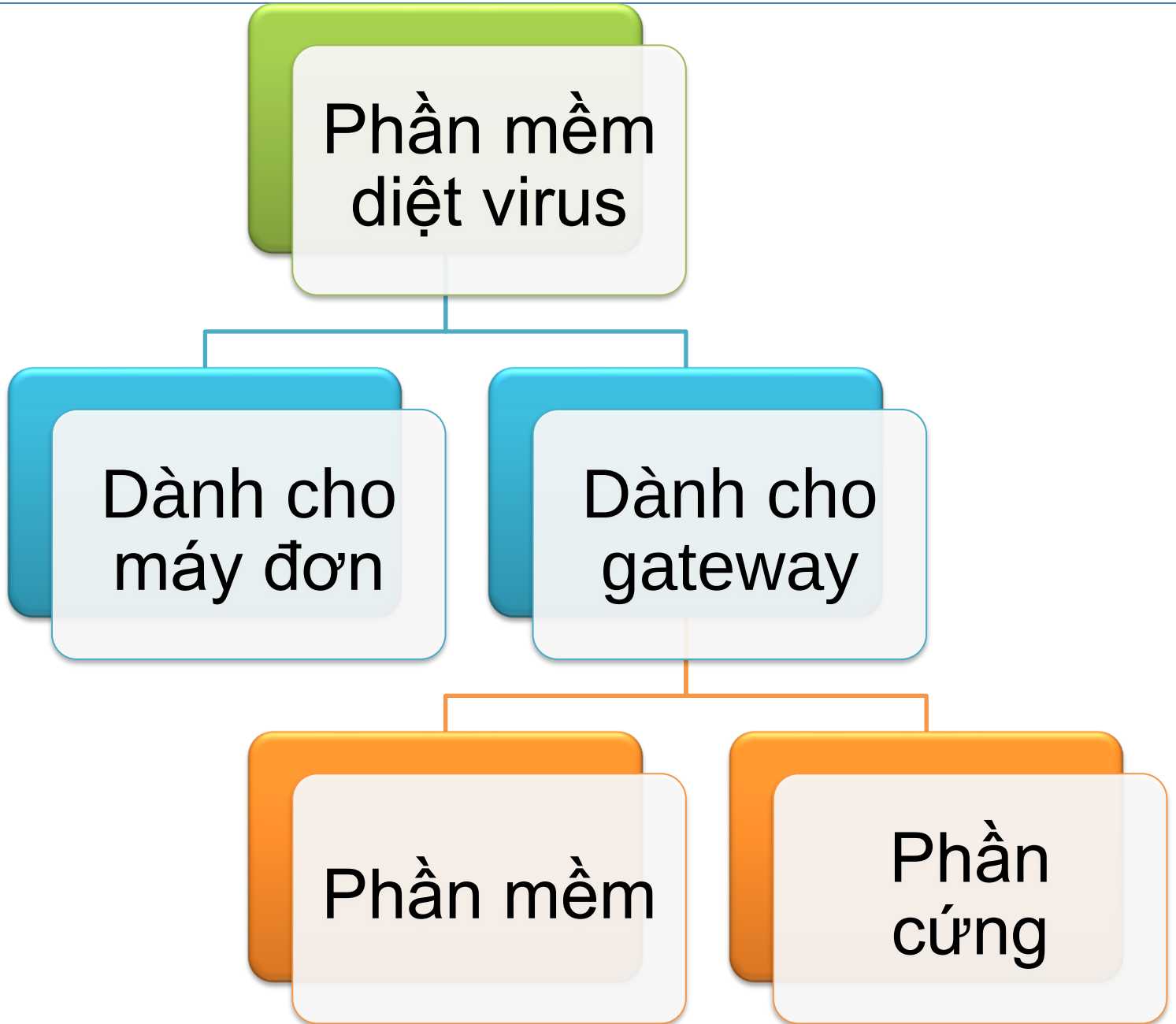
3 Phòng chống mã độc

Phòng chống mã độc

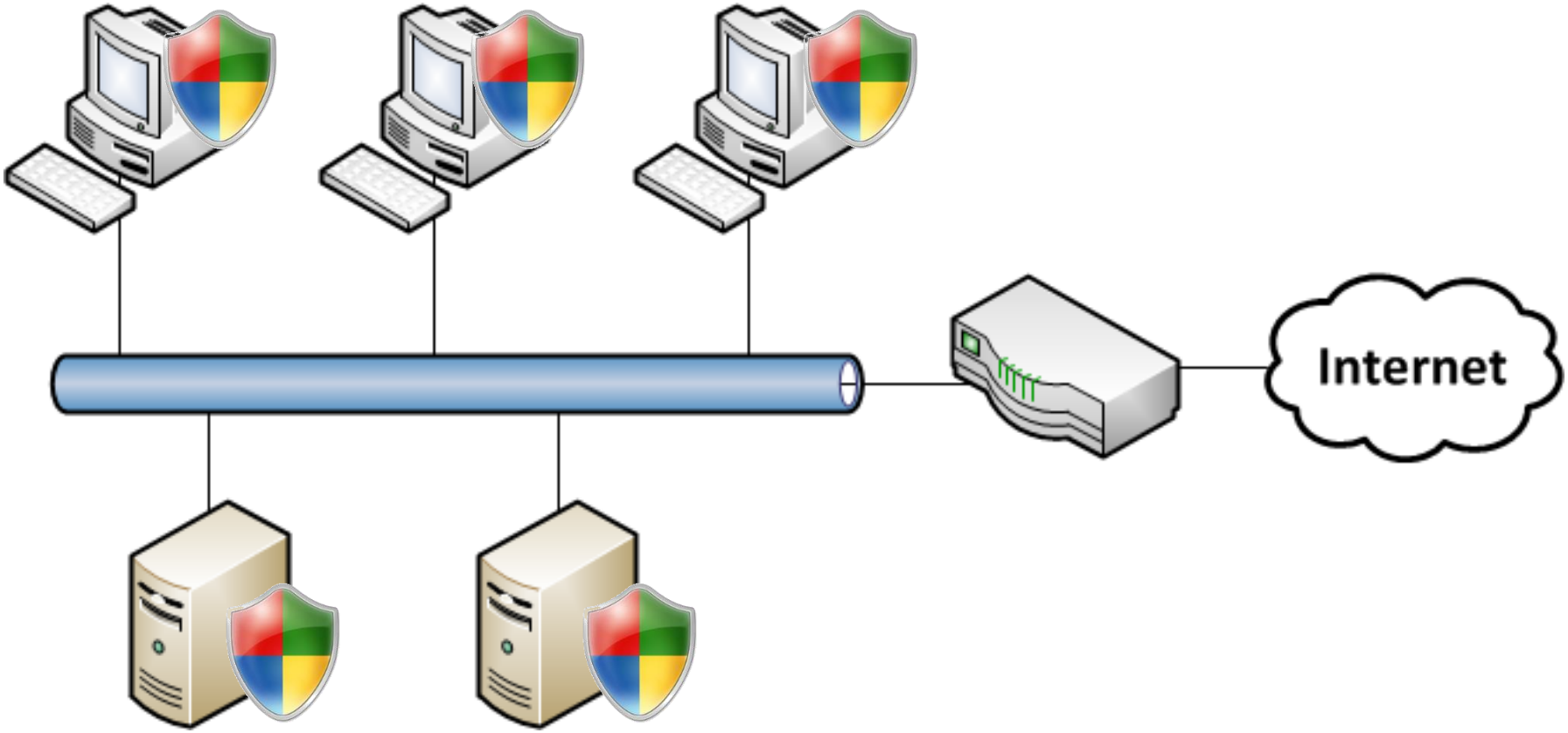
Phòng chống mã độc

- Công cụ diệt virus
- Kiểm tra phần mềm với www.virustotal.com
- Kiểm tra phần mềm qua chữ ký số
- Đóng băng ổ đĩa
- Sử dụng USB-AV
- Tuân thủ quy tắc an toàn

Công cụ diệt virus

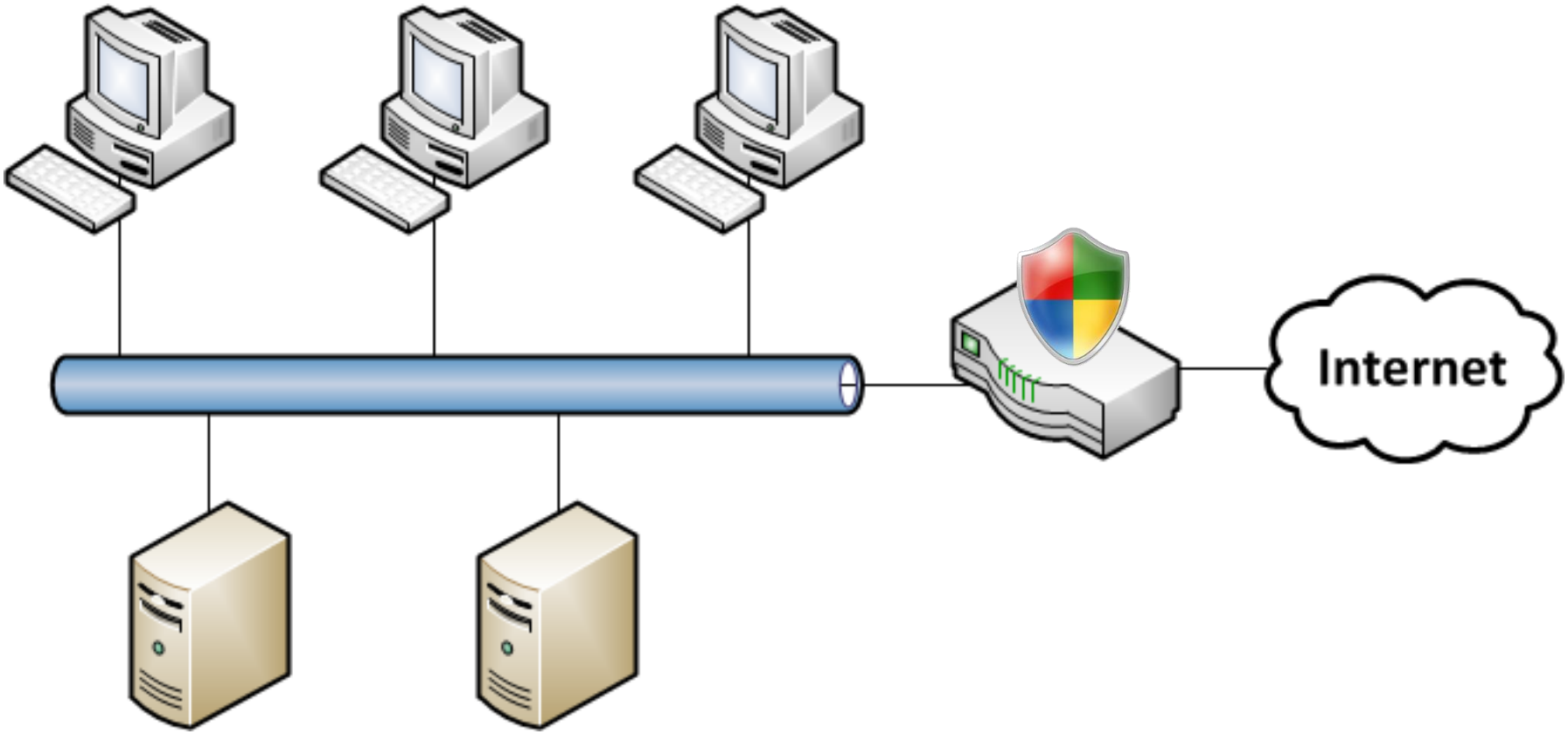


Diệt virus trên máy đơn



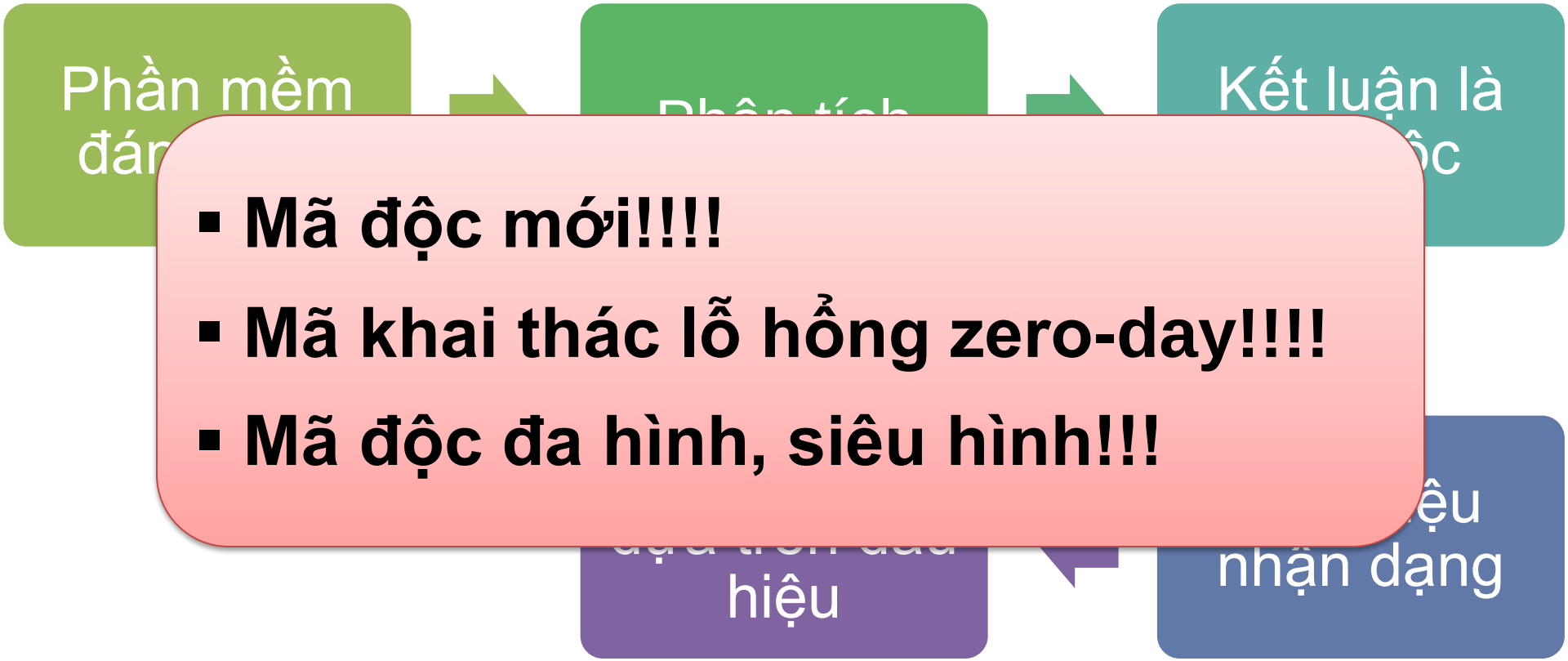
- Bảo vệ từ mọi hướng
- Phức tạp trong quản trị, cập nhật
- Có phiên bản dành cho doanh nghiệp

Diệt virus trên gateway



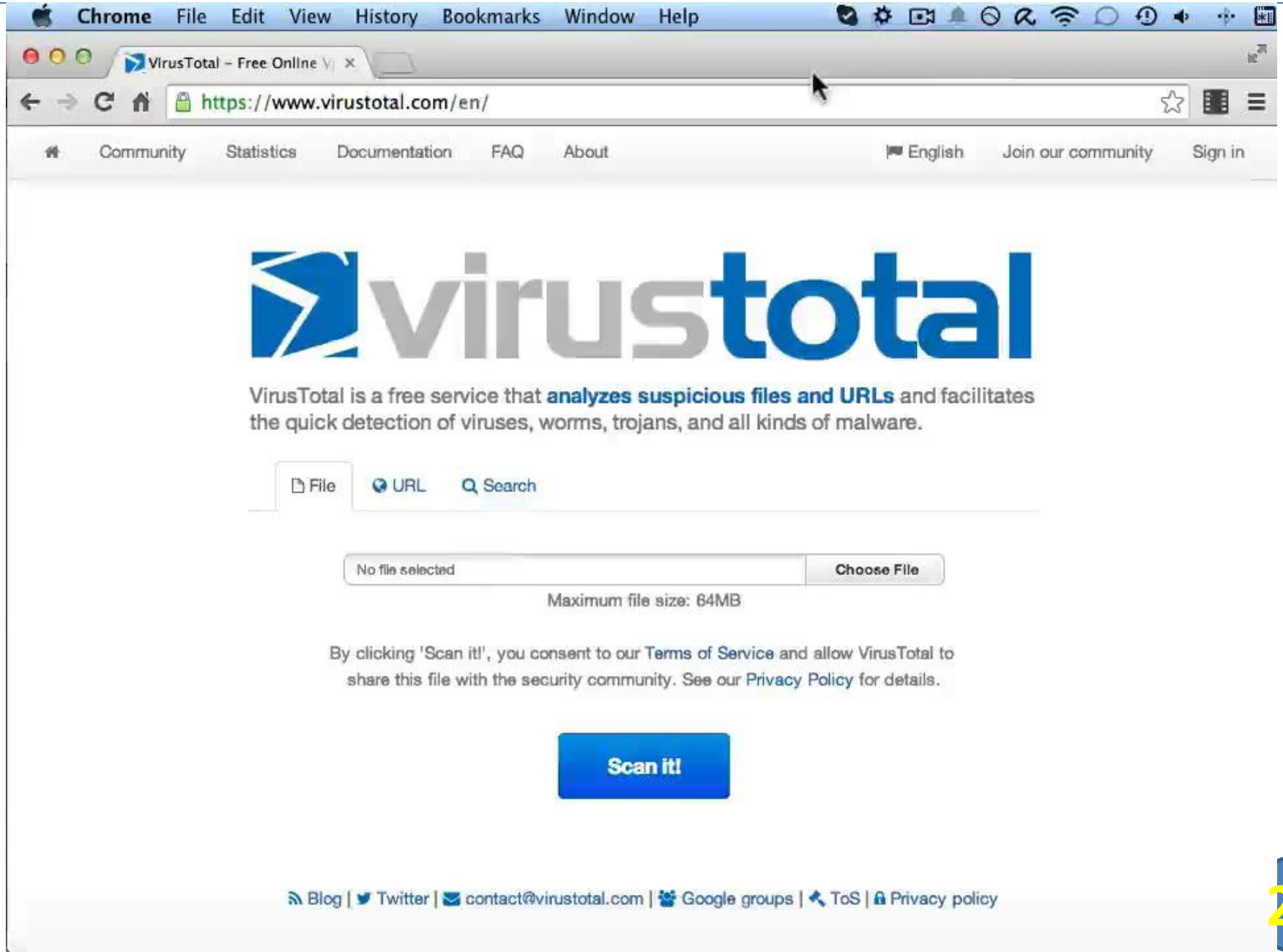
- Chỉ bảo vệ khi mã độc đến từ mạng ngoài
- Quản trị tập trung

Nhược điểm của chương trình diệt virus



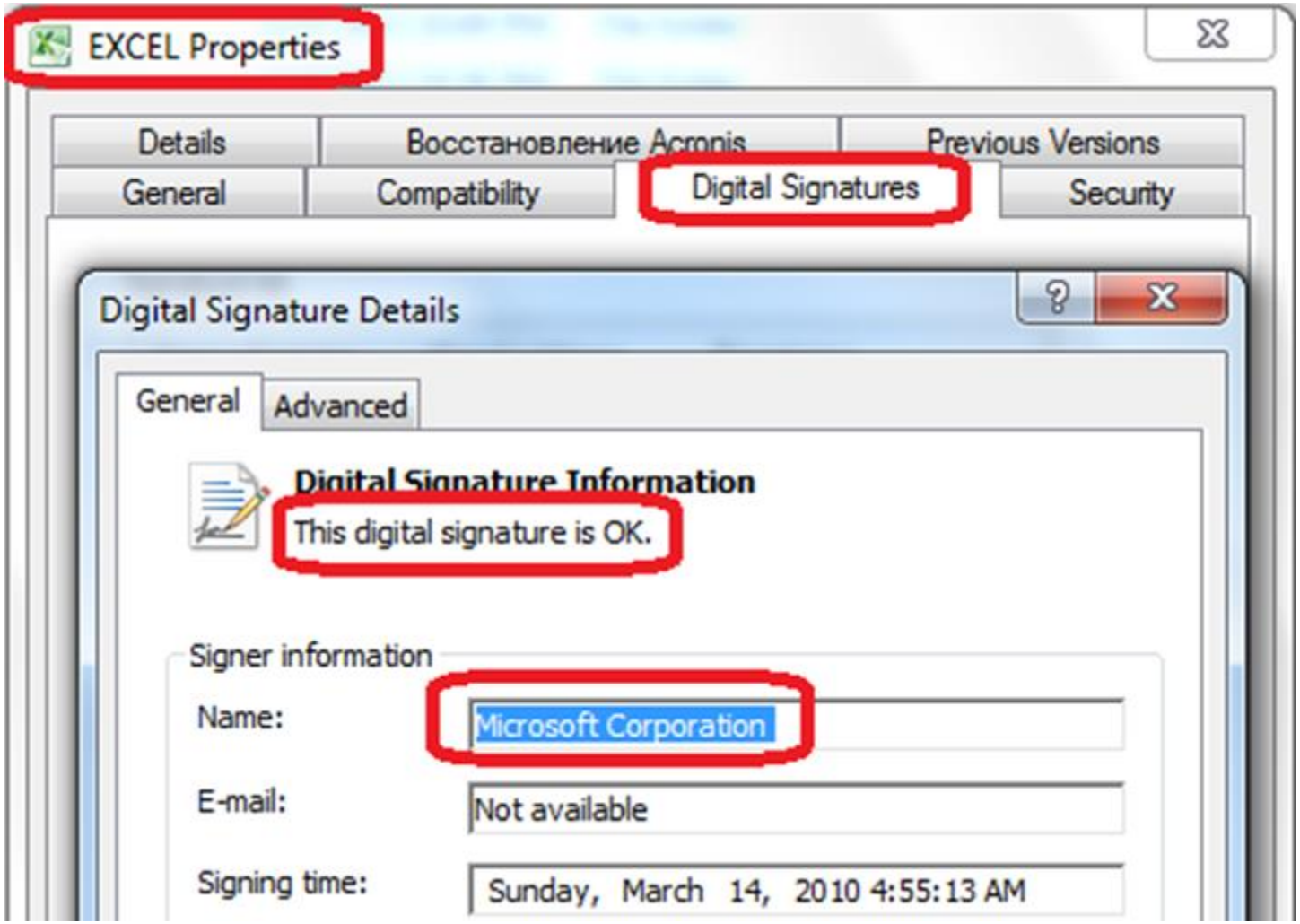
- **Mã độc mới!!!!**
- **Mã khai thác lỗ hổng zero-day!!!!**
- **Mã độc đa hình, siêu hình!!!**

www.virustotal.com



Phòng chống mã độc

❑Kiểm tra nguồn gốc phần mềm



Phòng chống mã độc

❑Đóng băng ổ đĩa

- Mọi thay đổi trên ổ đĩa chỉ có tác dụng khi máy đang chạy.
- Khi tắt hoặc khởi động lại máy, mọi thay đổi sẽ bị vô hiệu.
- Công cụ
  - Deep Freeze (Faronics Corporation)
  - Shadow Defender
  - Returnil Virtual System
  - Reboot Restore Rx (New Horizon)

Các quy tắc an toàn phòng chống virus (1/2)

- Không sử dụng các phần mềm không đáng tin cậy
- Quét virus cho thiết bị lưu trữ di động (USB, thẻ nhớ, ổ cứng cắm ngoài,....) trước khi sử dụng
- Hạn chế sử dụng thiết bị lưu trữ di động
- Cấm gửi/nhận các file nguy hiểm qua thư điện tử

Các quy tắc an toàn phòng chống virus (2/2)

- Không mở các file đính kèm từ email đáng ngờ (bao gồm cả email đến từ người quen biết)
- Không mở các đường link nhận được qua email, qua mạng xã hội, qua chat... (bao gồm cả đường link đến từ người quen biết)


Q
&
&
A

Tài liệu tham khảo

1. John Aycock, **Computer Viruses and Malware**, Springer, 2006
2. Ed Skoudis, **Malware: Fighting Malicious Code**, Prentice Hall, 2003
3. Michael Davis et.al., **Hacking Exposed: Malware & Rootkit Secrets & Solutions**, Mc Graw Hill, 2015
4. James M. Aquilina, et.al., **Malware Forensics: Investigating and Analyzing Malicious Code**, Syngress, 2008
5. Mihai Christodorescu et.al., **Malware Detection**, Springer, 2007