

TROJAN, BACKDOOR VIRUS VÀ WORM

Khoa Công nghệ thông tin và Truyền thông
Trường Đại học Cần Thơ

Phần B

VIRUS VÀ WORM

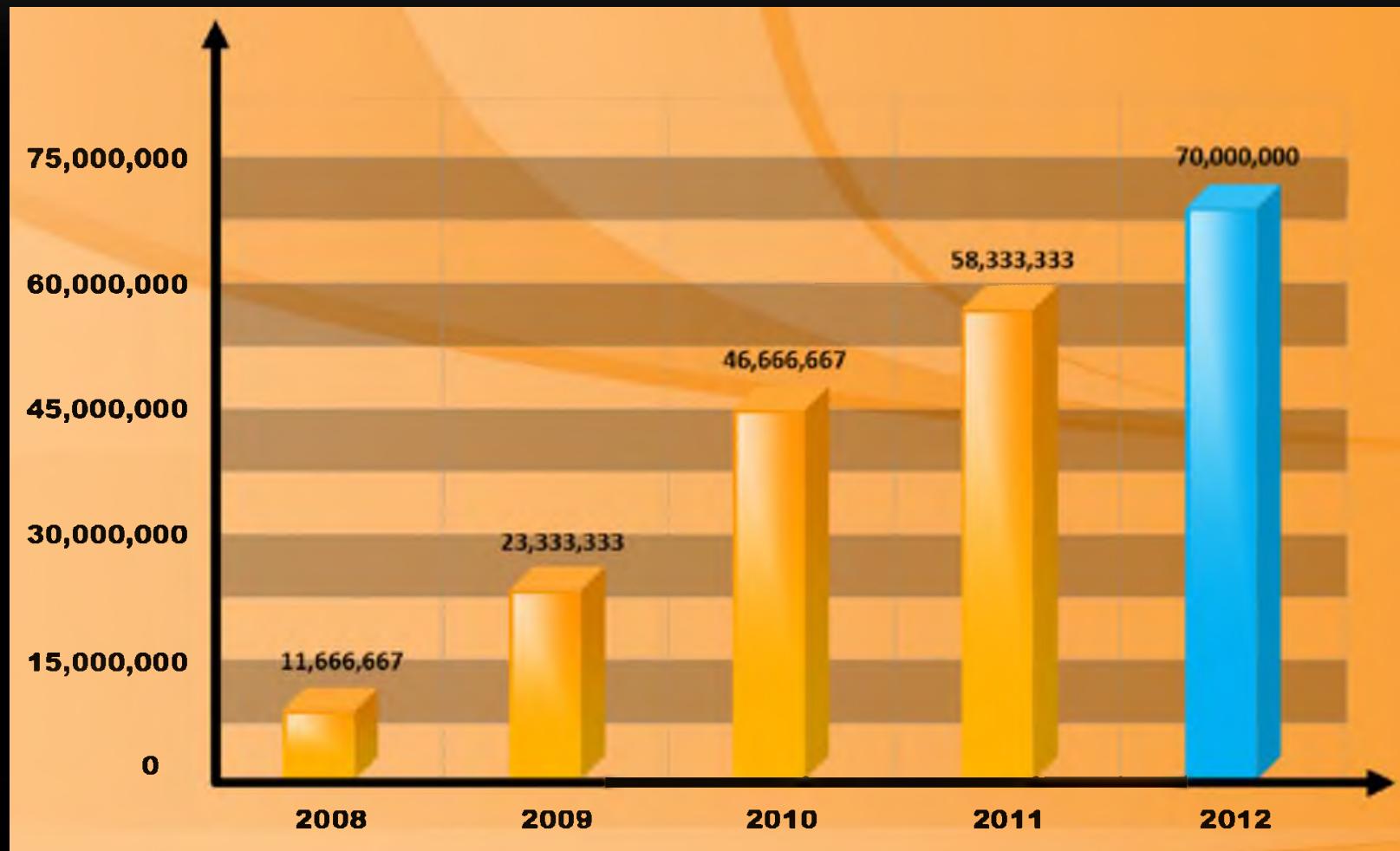
VIRUS VÀ WORM

- Virus và worm là gì.
- Các virus.
- Phương pháp phát hiện virus.
- Phòng chống virus.
- Tổng kết.

VIRUS VÀ WORM LÀ GÌ?

- Virus và worm đều là các phần mềm độc hại.
- Virus và worm có thể tự lây nhiễm và sửa đổi hệ thống để cho phép hacker truy cập vào.
- Virus và worm có thể mang Trojan và backdoor.
- Virus lây nhiễm vào một chương trình thực thi và sử dụng chương trình này để lây lan.
- Worm tương tự như virus nhưng có thể tự sao chép và di chuyển từ máy bị nhiễm sang máy khác.

THỐNG KÊ VỀ VIRUS VÀ WORM



VIRUS

- Virus là chương trình máy tính có thể tự nhân bản bằng cách tự gắn nó vào chương trình khác, boot record của máy tính hoặc các tài liệu có hỗ trợ lập trình script.
- Virus thông thường được lây nhiễm qua các tập tin mà nạn nhân tải về trên mạng, các đĩa bị nhiễm hoặc các tập tin đính kèm trong email.

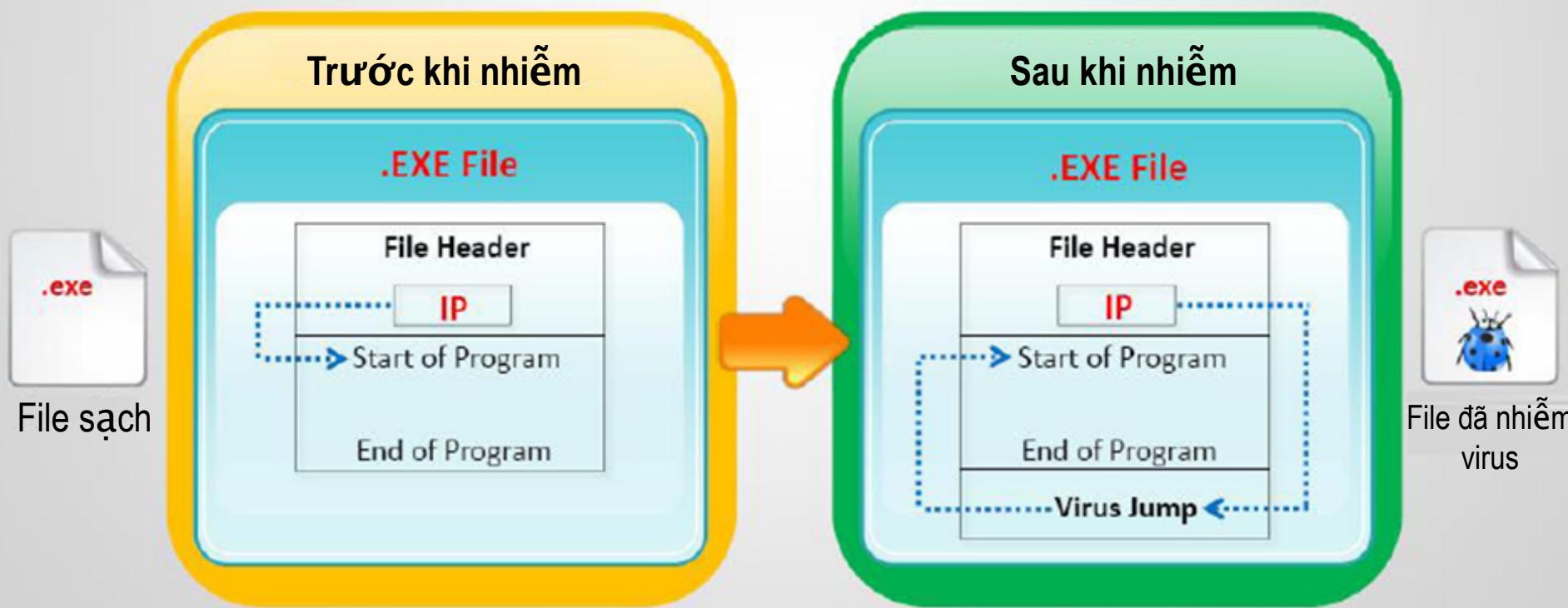
CÁC ĐẶC TÍNH CỦA VIRUS



VÒNG ĐỜI CỦA VIRUS



HOẠT ĐỘNG CỦA VIRUS: GIAI ĐOẠN LÂY NHIỄM



- Trong giai đoạn lây nhiễm, virus nhân bản nó và gắn bản sao vào một tập tin thực thi .exe trong hệ thống.

HOẠT ĐỘNG CỦA VIRUS: GIAI ĐOẠN TẤN CÔNG

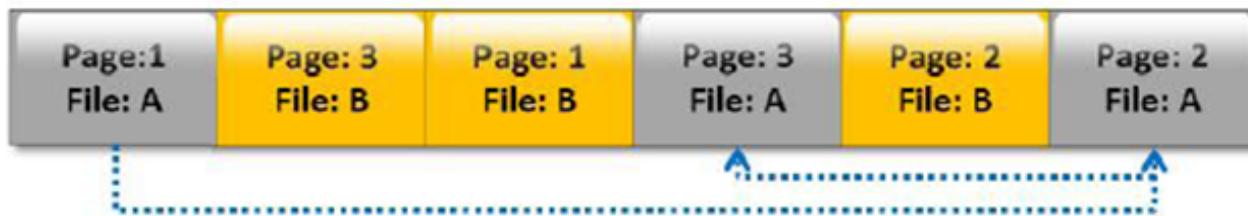
- Virus được lập trình để khi có sự kiện nào đó xảy ra thì nó sẽ tự kích hoạt và tấn công hệ thống.
- Một số virus tự kích hoạt khi chúng được chạy, một số khác sẽ tự kích hoạt khi một sự kiện nào đó xảy ra, ví dụ như: người dùng thực hiện một tác vụ nào đó, vào một ngày, một thời điểm nào đó...

HOẠT ĐỘNG CỦA VIRUS: GIAI ĐOẠN TẤN CÔNG

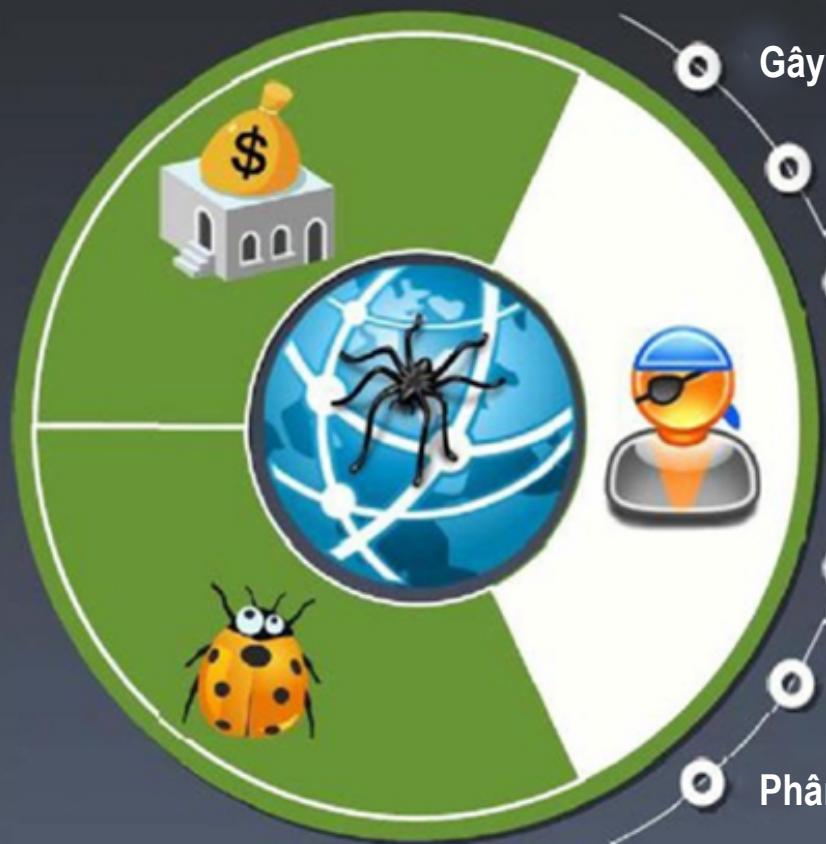
File chưa phân mảnh trước khi bị tấn công



File đã bị phân mảnh do sự tấn công của Virus



TẠI SAO NGƯỜI TA TẠO RA VIRUS



Gây thiệt hại cho đối thủ

Lợi ích kinh tế

Dự án nghiên cứu

Trò đùa

Phá hoại

Khủng bố mạng

Phân phát các thông điệp chính trị



Kẻ tấn công



Hệ thống có thể
công kích

DẤU HIỆU BỊ VIRUS TẤN CÔNG



Hoạt động bất thường

Nếu hệ thống hoạt động theo cách thức chưa từng thấy, bạn có thể nghi ngờ bị Virus tấn công



Lỗi thật sự

Tuy nhiên không phải tất cả các trực trặc có thể là do Virus tấn công

WORM MÁY TÍNH



Worm máy tính là chương trình độc hại có thể tái tạo thực thi và lây lan thông qua kết nối mạng một cách độc lập mà không tương tác với con người

Hầu hết Worm được tạo chỉ có thể tái tạo và lây lan thông qua mạng, tiêu thụ tài nguyên máy tính; tuy nhiên một vài Worm mang payload tàn phá hệ thống

Kẻ tấn công sử dụng Worm payload để cài đặt Backdoor vào máy tính bị nhiễm và tạo botnet; những botnet này có thể sử dụng để mang tấn công đến một không gian mạng nào đó

WORM KHÁC VIRUS NHƯ THẾ NÀO?

Worm là 1 dạng đặc biệt của Virus có thể tự nó tái tạo và sử dụng bộ nhớ, nhưng không thể tự nó tấn công chương trình khác



Worm lợi dụng file hoặc tính năng vận chuyển thông tin trên hệ thống máy tính và lây lan tự động thông qua mạng nhưng Virus thì không làm như vậy

PHƯƠNG PHÁP PHÁT HIỆN VIRUS

Quá trình phát hiện virus và loại bỏ như sau:

Phát hiện các cuộc tấn công dựa theo các dấu hiệu (trình bày ở trên)

Theo dõi quá trình sử dụng các tiện ích như handle.exe, listdlls.exe, fport.exe, netstat.exe và pslist.exe

Phát hiện payload virus bằng cách tìm kiếm các hành động thay đổi, thay thế, hoặc xóa các tập tin

Xác định các hướng lây nhiễm và cô lập nó. Sau đó, cập nhật các định nghĩa virus và quét lại toàn bộ hệ thống.

PHÒNG CHỐNG VIRUS

1

Tường lửa (firewall) kiểm soát dữ liệu ra vào máy tính và cảnh báo những hành vi đáng ngờ

2

Phần mềm chống virus

3

Cập nhật các bản sửa lỗi

4

Trình duyệt an toàn hơn

5

Suy nghĩ kỹ trước khi cài đặt một phần mềm nào đó

6

Sử dụng máy tính với quyền user

7

Sao lưu hệ thống

ĐỐI PHÓ VỚI VIRUS VÀ WORM

Đảm bảo file thực thi được gửi đến tổ chức đã được phê duyệt

Không boot máy tính với ổ đĩa bootable đã bị nhiễm

Hiểu biết về mối đe dọa Virus mới nhất

Kiểm tra CD và DVD có bị nhiễm hay không

Đảm bảo cửa sổ pop-up blocker được bật và sử dụng tường lửa internet



Chạy clean up ổ đĩa, quét registry và chạy chống phân mảnh 1 lần trong tuần

Bật tường lửa nếu OS sử dụng Windows

Chạy chương trình Anti virus 1 lần trong tuần

Chặn tất cả các file có phần mở rộng dài hơn phần mở rộng của file

Thận trọng với những file được gửi thông qua dòng tin nhắn tức thời

TỔNG KẾT

- Hiểu được virus và worm là gì, chúng lây lan và phá hoại như thế nào.
- Hiểu sự khác nhau giữa virus và worm
- Tìm hiểu các cách thức phòng-chống-ứng phó với sự lây nhiễm của virus và worm