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

7

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).

8

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.

9

Mã độc

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

10

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.

11

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. .

12

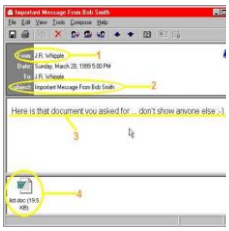
Lịch sử của mã độc

- Năm 1988: Virus Jerusalem xuất hiện, được kích hoạt vào thứ sáu ngày 13.
- Năm 1989: Xuất hiện chương trình Trojan có tên AIDS.

13

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.



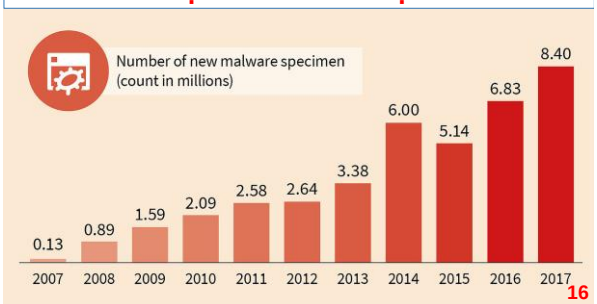
14

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.

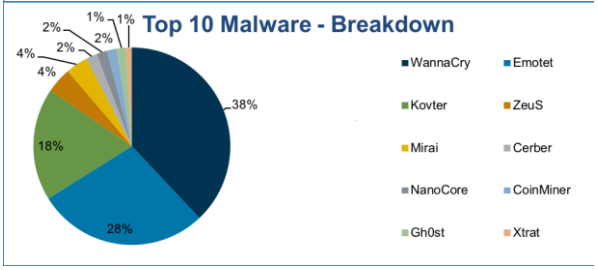
15

Lịch sử của mã độc



16

Lịch sử của mã độc



17

18

Mã độc

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

19

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…

20

Mã độc

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

21

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

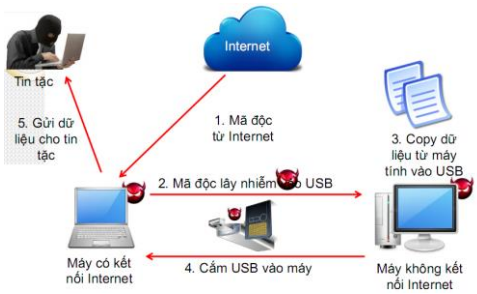
22

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

23

Qua các thiết bị lưu trữ di động



24

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.

25

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

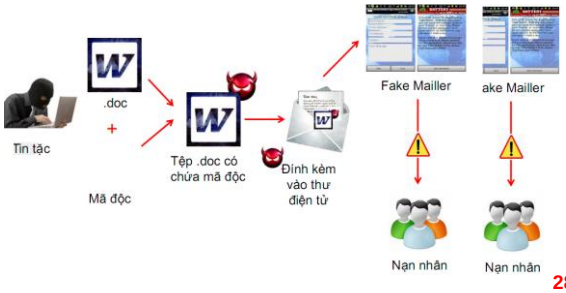
26

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

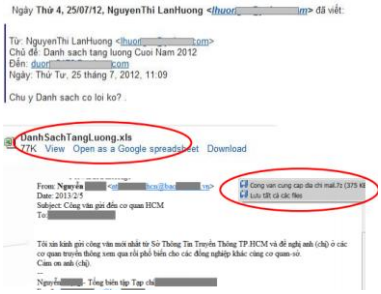
27

Qua thư điện tử



28

Qua thư điện tử



29

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

30

Quá trình duyệt web

31

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

32

Lây nhiễm từ smartphone sang máy tính

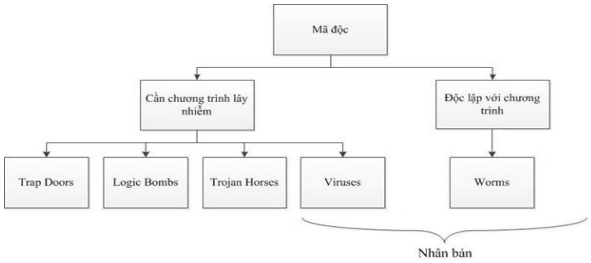
33

Nội dung

1. Mã độc
2. Phân loại mã độc
3. Cơ chế hoạt động của mã độc

34

Phân loại mã độc



35

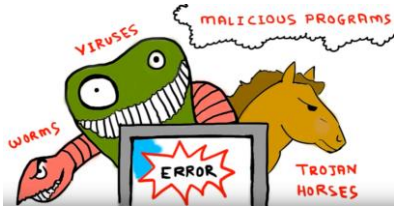
Nội dung

1. Mã độc
2. Phân loại mã độc
3. Cơ chế hoạt động của mã độc

36

Cơ chế hoạt động của mã độc

- Virus
- Worm
- Trojan horse



37

Cơ chế hoạt động của mã độc

- Virus
- Worm
- Trojan horse

38

Virus

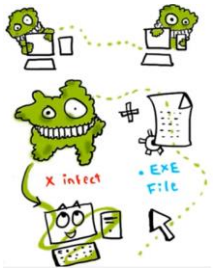
- Là một loại mã độc có khả năng tự nhân bản và lây nhiễm chính nó vào các tệp, chương trình máy tính.

39

Virus

Vòng đời virus gồm 4 giai đoạn:

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



40

Cơ chế hoạt động của mã độc

- Virus
- Worm
- Trojan horse

41

Worm

42

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:

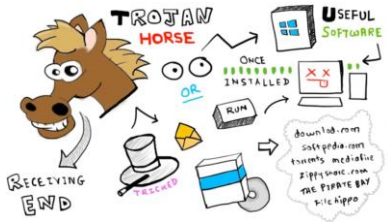
- Tìm kiếm các đối tượng phù hợp,
- Lây nhiễm,
- Tự sao chép bản thân nó vào các thư mục hệ thống đồng thời ghi thông tin khởi động vào hệ thống.

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

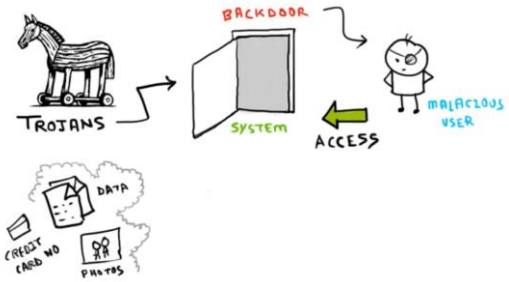


Trojan Horse

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**

49

Nội dung

1. **Mã độc**
2. **Phân loại mã độc**
3. **Cơ chế hoạt động của mã độc**

4