ĐẠI HỌC QUỐC GIA HÀ NỘI

BÀI GIẢNG
TIN HỌC CƠ SỞ
(Được thực hiện trong dự án eBook)

NỘI DUNG

- Phần mềm xấu
- Các hoạt động có mục đích xấu
- Những vấn đề pháp lý về CNTT

BÀI 12. AN NINH THÔNG TIN

Giảng viên: ĐÀO KIẾN QUỐC
Email: dkquoc@vnu.edu.vn

PHẦN MỀM XẤU (malware)

- Phần mềm xấu là phần mềm gây các tác động xấu
- Một số loại phần mềm xấu
  - Virus và worm: phần mềm xấu có khả năng lây lan. Sự khác nhau giữa virus và worm chủ yếu là hình thức tồn tại và cơ chế lây lan
  - Trojan: phần mềm xấu có hoạt động nội gián, khi bị cài đặt (bằng cơ chế của virus, hay người dùng do thiếu hiểu biết tự cài đặt) nó sẽ thực hiện những hoạt động gián điệp

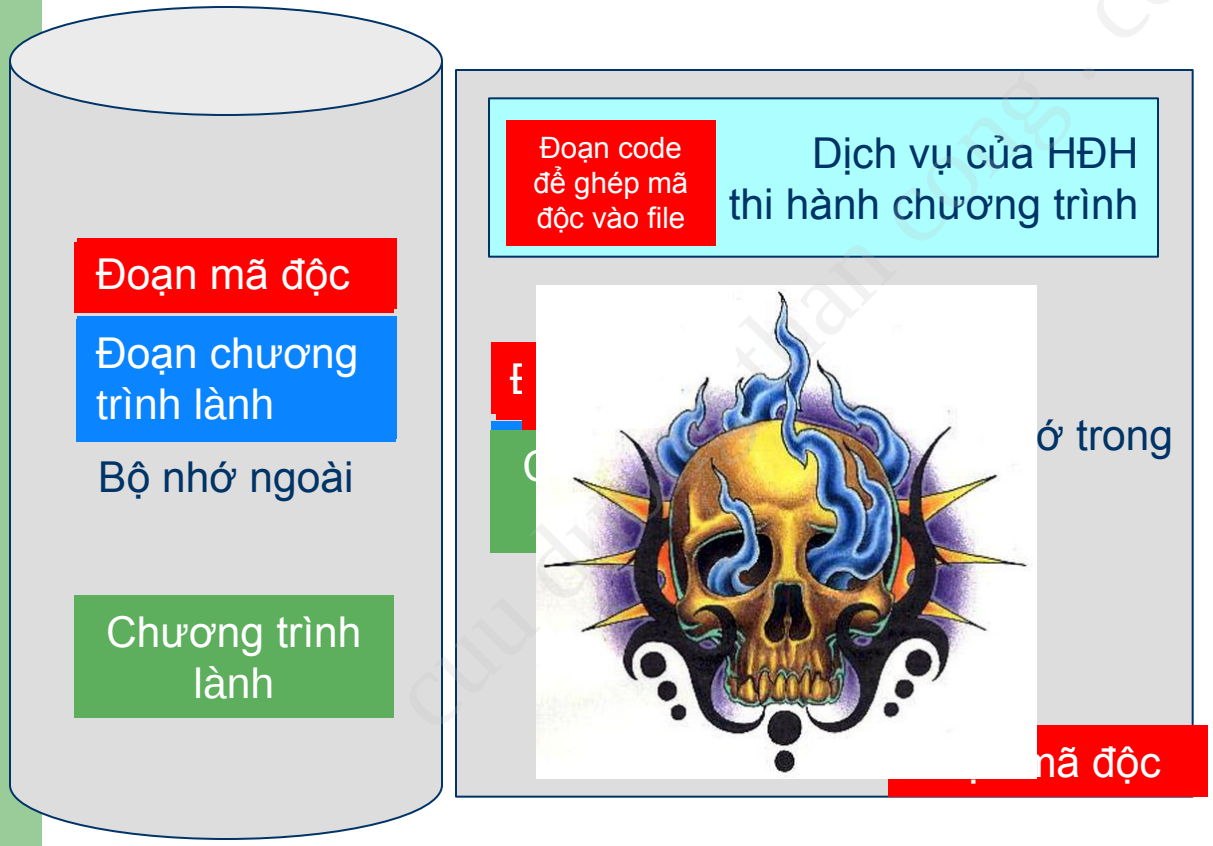
VIRUS VÀ SÂU (WORM)

Virus là các đoạn mã chương trình có mục đích xấu có các đặc tính sau:

- Tương đối nhỏ, hiệu quả cao và thường có các cơ chế chống phát hiện.
- Tồn tại bằng cách ghép vào một vật chủ như một file (virus file) hay vào đoạn mã khởi động của hệ điều hành (virus boot).
- Có khả năng lây lan, khi nhiễm, nó chiếm quyền điều khiển của hệ điều hành để tự nhân bản nhằm lây lan từ file này sang file khác hoặc từ máy này sang máy khác
- Cơ chế tồn tại và lây lan giống với virus sinh học

- Sâu là chương trình độc lập, hoàn chỉnh không cần gắn vào vật chủ là file hay bộ nhớ ngoài.
- Sâu lây lan theo đường mạng
- Tuy nhiên khi nói về virus nói chung người ta vẫn hàm ý nói cả virus và worm.

CƠ CHẾ LÂY NHIỄM CỦA VIRUS FILE



Thi hành CT nhiễm Virus

- Nạp CT vào BN
- Chạy
  - Chạy đoạn mã độc
  - Sửa dịch vụ thi hành
  - Sao mã độc ra BN
  - Gây hiệu ứng xấu
  - Chạy đoạn mã lành
- Thực hiện xong, máy bị nhiễm virus

Thi hành CT lành từ máy bị nhiễm VR

- Nạp CT vào BN
- Chạy
  - Thi hành đoạn mã độc sửa đổi
  - Kiểm tra nếu file chưa nhiễm thì ghép mã độc vào file, hoàn thành lây nhiễm
  - Thi hành mã lành

CƠ CHẾ LÂY VIRUS BOOT

Có nhiều điểm tương đồng với cơ chế lây của virus file

Đọc đĩa nhiễm Virus

- Nạp đĩa
- Khởi động đĩa
  - Chạy đoạn khởi động
  - Sửa dịch vụ ghi đĩa
  - Sao mã độc ra BN
  - Gây hiệu ứng xấu
  - Chạy đoạn khởi động
- Khởi động xong, máy bị nhiễm virus

Thi hành CT nhiễm Virus

- Nạp CT vào BN
- Chạy
  - Chạy đoạn mã độc
  - Sửa dịch vụ thi hành
  - Sao mã độc ra BN
  - Gây hiệu ứng xấu
  - Chạy đoạn mã lành
- Thực hiện xong, máy bị nhiễm virus

Đọc đĩa lành từ máy bị nhiễm VR

- Nạp đĩa
- Chạy khởi động đĩa
  - Thi hành đoạn mã độc sửa vùng boot
  - Kiểm tra nếu đĩa chưa nhiễm thì ghép mã độc vào boot, hoàn thành lây nhiễm
  - Thi hành mã lành

Thi hành CT lành từ máy bị nhiễm VR

- Nạp CT vào BN
- Chạy
  - Thi hành đoạn mã độc sửa đổi
  - Kiểm tra nếu file chưa nhiễm thì ghép mã độc vào file, hoàn thành lây nhiễm
  - Thi hành mã lành

CƠ CHẾ SỐNG VÀ LÂY NHIỄM CỦA VIRUS BOOT

- Khi khởi động máy tính từ một thiết bị nhớ ngoài bị nhiễm virus, máy tính thi hành đoạn mã nạp hệ điều hành ở vùng boot, đoạn mã độc sẽ được thi hành để làm những việc sau:
  - Tải đoạn mã độc vào bộ nhớ
  - Sửa chức năng đọc và ghi đĩa của hệ điều hành
  - Thi hành chức năng xấu trong đoạn mã độc hại
- Khởi động xong đoạn mã độc sẽ có sẵn trong bộ nhớ, còn chức năng đọc đĩa của HĐT đã bị thay đổi
- Khi đặt một thiết bị nhớ ngoài mới vào máy chức năng mới thi hành chương trình của HĐH sẽ làm :
  - Kiểm tra bộ nhớ ngoài mới đã nhiễm virus chưa
  - Nếu chưa, sửa lại boot bằng cách ghép mã độc ở bộ nhớ

CÁCH PHÁT TÁN CỦA SÂU

- Sâu phát tán được do bất cẩn của người dùng như tải file về từ Internet qua email hay bấm vào một đường link trên web. Người phát tán thường bẫy các link này hay gửi theo email
- Một số sâu chủ động khai thác lỗ hổng bảo mật của các máy chủ (như Code Red hay Nimda)
- Khi xâm nhập vào máy, một số sâu có hành động phát tán như tìm các địa chỉ email trong máy bị nhiễm, gửi thư với danh tính của chủ máy đính kèm chính sâu này hoặc bẫy các đường link để người nhận thư mắc bẫy
- Tốc độ phát tán qua mail của một số virus rất lớn

TROJAN (Con ngựa thành Troia)

- Lấy tên từ điển tích văn học Con ngựa thành Troia (Trojan Horse) của quân Hy lạp
- Trojan là các phần mềm xấu được cài theo cơ chế lây nhiệm của virus, worm hoặc lừa để người dùng tự cài đặt.
- Một số dạng thức hoạt động nội gián:
  - Spyware : ăn trộm thông tin như tài khoản để báo ra ngoài
  - Một dạng spyware: keylogger ghi lại bàn phím đã được gõ thế nào để chuyển ra ngoài
  - Backdoor: mở ra một cổng sau để chủ có thể truy cập ngầm vào máy tính bị nhiễm.
  - Một dạng backdoor: Rootkit chiếm quyền điều khiển để có thể truy cập và xóa hết mọi dấu vết. Rootkit cũng là một loại backdoor

MỘT SỐ HOẠT ĐỘNG CÓ MỤC ĐÍCH XẤU

- Tấn công trực tiếp hoặc xâm phạm các hệ thống thông tin như lấy trộm tài khoản, tạo ra và phát tán vi-rút, vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính gây rối loạn hoạt động, phong toả hoặc lấy cắp thông tin, làm biến dạng, làm huỷ hoại các dữ liệu của máy tính, tấn công từ chối dịch vụ (DoS)
- Lạm dụng mạng máy tính để phạm tội như lừa đảo qua mạng; phát tán các tài liệu phản văn hoá, vi phạm an ninh quốc gia; sử dụng Internet để nhằm mục đích đe doạ, quấy rối, xúc phạm đế danh dự, nhân phẩm của người khác
- Vi phạm tính riêng tư qua thư rác (Spamming) và phần mềm quảng cáo (Adware)

MẠO DANH, XÂM NHẬP TRÁI PHÉP

- Ăn cắp mật khẩu bảng cách thử tự động một cách có hệ thống
- Bằng lừa đảo những người cả tin, nhẹ dạ
- Ăn trộm mật khẩu bằng cách bắt các gói tin của mạng để phân tích (sniffer).
- Dùng các phần mềm gián điệp (Spyware). Phần mềm được gửi qua mail hay kích thích để người sử dụng download về chạy thử. Khi chạy một lần là bị nhiễm. Phần mềm này sẽ gửi các thông tin của máy ra ngoài giúp cho tin tặc có thể khống chế được máy bị nhiễm.
- Một loại phần mềm spyware là Keylogger

TẤN CÔNG TỪ CHỐI DỊCH VỤ (DOS)

- DOS (Denial of Service) là loại hình tấn công khiến hệ thống không thể đáp ứng được yêu cầu dịch vụ nữa. Có 2 hình thái tấn công chính :
  - Tiêu hao tài nguyên tính toán (như băng thông đường truyền, không gian đĩa, chiếm dụng thời gian CPU).
  - Phá vỡ thông tin cấu hình của hệ thống khiến hệ thống từ chối dịch vụ (chẳng hạn làm sai lạc hệ thống DNS)
- Hình thức tiêu hao tài nguyên chính hiện nay là tạo mạng ma (botnet) với các máy tính nhiễm phần mềm tấn công gọi là âm binh (zombie)
  - Dùng virus hoặc worm để cài đặt phần mềm tấn công (tạo các zombie)
  - Các zombie mỗi khi nối mạng sẽ truy cập đến máy chỉ huy. Nếu có lệnh tấn công nó sẽ gửi liên tiếp các yêu cầu truy cập với tần số cực lớn như gửi mail, tra cứu web, ping, yêu cầu xác nhận… làm máy chủ bị quá tải

SỬ DỤNG MẠNG MÁY TÍNH VÌ CÁC MỤC ĐÍCH XẤU

- Phát tán các tài liệu văn hoá đồi truỵ, các tài liệu có hại cho an ninh, các tài liệu kích động tư tưởng dân tộc hẹp hòi, xung đột tôn giáo và bạo lực
- Lừa đảo qua mạng (phishing/biến thể của fishing) đưa ra mồi bẫy để dụ người dùng tiết lộ thông tin hoặc tạo các website giả lôi kéo người dùng để lừa đảo về mặt kinh tế
- Đe doạ, quấy rối, đưa tin thất thiệt, xúc phạm người khác qua mạng

VI PHẠM TÍNH RIÊNG TƯ

- Công bố hình ảnh, tin tức của cá nhân không được phép
- Thư, tin nhắn rác. 1/3 lượng thư trên toàn cầu là thư rác tiêu tốn tài nguyên Internet và gây khó chịu cho người nhận
- Đã có nhiều giải pháp công nghệ chống spam nhưng không thể chống triệt để
- Đã có đạo luật chống spam nhưng thi hành còn khó
- Đã có

MỘT SỐ ĐIỀU KHOẢN TRONG BỘ LUẬT HÌNH SỰ VỀ TỘI PHẠM TIN HỌC

- Điều 224. Tội tạo ra và lan truyền, phát tán các chương trình virus
- Điều 225. Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử
- Điều 226. Tội sử dụng trái phép thông tin trên mạng và trong máy tính
- Nghị định 55/2001/NĐ-CP, điều 41 quy định một số mức xử phạt các vi phạm khi sử dụng Internet chưa đến mức hình sự
  - Khoản 2 về Sử dụng mật khẩu, khoá mật mã, thông tin riêng của người khác để truy nhập, sử dụng dịch vụ Internet trái phép và sử dụng các công cụ phần mềm để truy nhập, sử dụng dịch vụ Internet trái phép"
  - Khoản 5 về Sử dụng Internet để nhằm mục đích đe doạ, quấy rối, xúc phạm đế danh dự , nhân phẩm của người khác; Đưa vào Internet hoặc lợi dụng Internet để truyền bá các thông tin, hình ảnh đồi truy, hoặc những thông tin khác trái với quy định của pháp luật về nội dung thông tin trên Internet; Đánh cắp mật khẩu, khoá mật mã, thông tin riêng của tổ chức, cá nhân và phổ biến cho người khác sử dụng; Vi phạm các quy định về vận hành, khai thác và sử dụng máy tính gây rối loạn hoạt động, phong toả hoặc làm biến dạng, làm huỷ hoại các dữ liệu trên Internet
  - Khoản 6 về tạo ra và cố ý lan truyền, phát tán các chương trình vi rút trên Internet

HẾT BÀI 15. AN NINH THÔNG TIN

CẢM ƠN ĐÃ THEO DÕI BÀI GIẢNG