**Bài 2b. Các phần mềm gây hại – Virus**

**1) Tổng quan về Virus máy tính**

- Là một phần mềm có thể sao chép chính nó. Nó không đứng một mình mà phải gắn vào một tập tin hoặc một chương trình khác.

- Chương tình Virus thường thực hiện các bước sau:

+ Tìm cách gắn vào đối tượng chủ, sửa dữ liệu sao cho virus nhận được quyền điều khiển mỗi khi chương trình chủ được thực thi.

+ Khi thực hiện, virus tìm kiếm những đối tương khác, sau đó lây nhiễm lên những đối tượng này.

+ Tiến hành những hoạt động phá hoại, do thám.

+ Trả lại quyền thi hành cho chương trình chủ hoạt động như bình thường.

- Virus máy tính và mạng máy tính

+ Có khả năng sử dụng những tính năng của hệ điều hành/ứng dụng để truyền bá, lây nhiễm trên mạng => Khả năng lây lan nhanh chóng và rộng rãi.

+ Có khả năng tiến hành những hoạt động phá hoại, do thám trên mạng máy tính, gây ảnh hưởng nghiêm trọng đế sự ổn định, tin cậy và an toàn của mạng.

- Tính chất của Virus máy tính:

+ Tính lây lan

+ Tính phá hoại

+ Tính nhỏ gọn

+ Tính tương thích

+ Tính phát triển kế thừa

- Phân loại:

+ Qua phương pháp tìm đối tượng lây nhiễm:

1. Virus thường trú
2. Virus không thường trú

+ Qua đối tượng lây nhiễm và môi trường hoạt động:

1. Boot Virus
2. File-System Virus
3. File-Format Virus
4. Macro Virus
5. Script Virus
6. Registry Virus

+ Qua phương pháp lây nhiễm:

1. Ghi đè
2. Ghi đè bảo toàn
3. Dịch chuyển
4. Song hành
5. Nối thêm
6. Chèn giữa
7. Định hướng lại lệnh nhảy
8. Điền khoảng trống

+ Một cach phân loại khác:

1. System Secctor or Boot Virus: Lây nhiễm trên cùng boot của đĩa.
2. File Virus: Lây nhiễm trên các file thực thi.
3. Macro Virus: Lây nhiễm trên các tập tin word, excel, access, …
4. Source Code Virus: ghi code của Trojan đè hoặc nối tiếp vào code của tập tin chủ.
5. Network Virus: tự phát tán theo email bằng cách sử dụng lệnh và các giao thức của mạng máy tính.
6. Stealth: ẩn với các chương trình chống virus.
7. Polymorphic Virus: thay đổi đặc điểm của nó với mỗi lần lây nhiễm.
8. Cavity Virus: duy trì kích thước file không thay đổi trong khi lây nhiễm.
9. Tunneling Virus: tự che giấu dưới những dạng anti-virus khi lây nhiễm.
10. Camouflage Virus: ngụy trang dưới dạng những ứng dụng chính hãng của người dùng.
11. Shell Virus: mã tạo thành 1 shell xung quanh mã của chương trình bị nhiễm, như 1 chương trình con trên chương trình gốc nguyên thủy.
12. Add-on Virus: ghi mã nối tiếp vào điểm bắt đầu của chương trình bị nhiễm và không tạo thêm thay đổi nào.
13. Intrusive Virus: viết đè đoạn code của nó lên một phần hoặc hoàn toàn code của file bị nhiễm.

-Các loại Virus:

+ Virus hệ thống hoặc khu vực khởi động. + Virus đồng hành/ Virus ngụy trang

+ Virus đánh cắp/ virus đào hầm + Virus vỏ bọc

+ Virus mã hóa + Virus mở rộng tập tin

+ Virus đa hình + Virus da phân

+ Virus sửa lại file hoặc virus khoan lỗ + Virus vĩ mô

+ Virus trong file + Virus bổ sung.

+ Virus cụm + Virus xâm phạm

+ Virus lây nhiễm thưa thớt + Virus hành động trực tiếp hoặc thoáng qua

+ Virus thường trú

-Một số Virus phổ biến:

+ I love you virus. (worm, malware)

+ Klez Virus (worm)

+ W32/Divvi

+ Disk Killer

-Worm:

+ Sâu máy tính là các chương trình độc hại có khả năng sao chép, thực thi và lây lan trên các kết nối mạng một cách độc lập mà không cần sự tương tác của côn người.

+ Hầu hết các sâu được tạo ra chỉ để sao chép và lây lan qua 1 mạng, tiêu thụ tài nguyên có sẵn của máy, tuy nhiên, một số sâu mang tải trọng gây hại cho hệ thống máy chủ.

+ Người tấn công sử dụng tải trọng của sâu để cài đặt cửa sau vào máy tính bị nhiễm, biến chúng thành zombie để tạo một mạng botnet được sử dụng để thực hiện thêm các cuộc tấn công mạng.

-Sự khác nhau của sâu và Virus:

+ Sâu là một loại phần mềm độc hại đặc biệt có thể tự sao chép và sử dụng bộ nhớ nhưng không thể tự gắn vào các chương trình khác.

+ Sâu tận dụng tính năng truyền tải tệp hoặc thông tin trên hệ thống máy tính và tự động lây lan qua mạng bị nhiễm còn virus thì không.

1. **Các kỹ thuật của Virus máy tính**

- Các kĩ thuật cơ bản:

+ Kỹ thuật lây nhiễm:

1. Kĩ thuật cơ bản phải có ở virus, đơn giản hay phức tạp tùy loại.
2. Kĩ thuật lây nhiễm Boot Record / Master Boot của đĩa: thay thế BR hoặc MB trên phân vùng hoạt động với chương trình Virus.
3. Kĩ thuật lây nhiễm file thi hành: chương trình virus sẽ được ghép vào file chủ bằng cách nối thêm, chèn giữa, điền vào khoảng trống, ghi đè…
4. Thuật toán thường dùng để lây nhiễm một file .COM:

# Mở file

# Ghi lại thời gian/ ngày tháng/ thuộc tính

# Lưu trữ các byte đầu (thường là 3 bytes)

# Tính toán lệnh nhảy mới

# Đặt lệnh nhảy

# Chèn thân virus chính vào

# Khôi phục thời gian/ ngày tháng/ thuộc tính

# Đóng file

+ Kỹ thuật định vị trên vùng nhớ:

1. Phân phối một vùng nhớ để thường trú, chuyển toàn bộ chương trình virus tới vùng nhớ này, sau đó chuyển quyền điều khiển cho đoạn mã tại vùng nhớ mới với địa chỉ segment: offset mới.
2. Kỹ thuật quan trọng đối với các chương trình virus dạng mã máy (virus Boot, virus file). Virus macro và virus Script thực chất là các lệnh của chương trình ứng dụng nên không cần tiến hành kỹ thuật này.

+ Kỹ thuật kiểm tra sự tồn tại:

1. Mỗi virus chỉ nên lây nhiễm/kiểm soát một lần để đảm bảo không làm ảnh hưởng đến tốc độc làm việc của máy tính.
2. Virus phải kiểm tra sự tồn tại của chính mình trước khi lây nhiễm hoặc thường trú. (kiểm tra trên đối tượng bị lây nhiễm, kiểm tra trên bộ nhớ).
3. Kỹ thuật kiểm tra thường là:

# Dò tìm đoạn mã nhận diện trên file hoặc bộ nhớ.

# Kiểm tra theo kích thước hoặc nhãn thời gian của file.

+ Kỹ thuật thường trú:

1. Virus Boot phải phân phối một vùng nhớ riêng để lưu giữ chương trình virus bao gồm mã lệnh, biến, vùng đệm.
2. Các virus file cần phải kiểm tra xem chương trình đã thường trú chưa, nếu chưa sẽ định rõ vùng nhớ muốn sử dụng, copy phần virus vào bộ nhớ, sau đó khôi phục file chủ và trả quyền điều khiển về cho file chủ.

+ Kỹ thuật mã hóa: Che giấu mã lệnh thực sự của chương trình virus. Thủ tục mã hóa cũng chính là thủ tục giải mã.

+ Kỹ thuật ngụy trang:

1. Giấu, ngụy trang virus trên đối tượng chủ.
2. Virus sử dụng kĩ thuật này thường chậm bị phát hiện nên có khả năng không lây lan mạnh.

+ Kỹ thuật phá hoại: Đa dạng, phá hoại dữ liệu trên máy tính hoặc phá hỏng 1 phần máy tính

+ Kỹ thuật chống bẫy:

1. Chọn lọc file trước khi lây nhiễm theo một số tiêu chí nào đó nhằm tránh những file bẫy của chương trình Antivirus.

# Không lây nhiễm các file có số trong tên file

# Không lây nhiễm những chương trình sử dụng nhiều mã lệnh đặc biệt.

# Không lây nhiễm các file có tên liên tục (Vd: aaaaaa.com…).

# Không lây nhiễm các file liên tục có cùng kích thước.

# Không lây nhiễm các file ở thư mục gốc.

# Không lây nhiễm các file có lệnh nhảy và lệnh gọi zero.

#...

+ Kỹ thuật tối ưu: Gồm các kỹ thuật viết mã và thiết kế nhằm tối ưu chương trình về tốc độ và kích thước.

+ Các kỹ thuật đặc biệt:

1. Kỹ thuật tạo vỏ bọc: chống gỡ rối/ dịch ngược mã virus chống lại antivirus
2. Kỹ thuật đa hình: chống các phương pháp dò tìm mã mà antivirus dùng để nhận dạng virus bằng cách tạo ra các bộ giải mã khác biệt.
3. Kỹ thuật biến hình: chống lại chương trình antivirus bằng cách tạo đoạn mã mới hoàn toàn.
4. Kỹ thuật chống mô phỏng: chống lại phương pháp heuristic dựa trên hành vi của chương trình bằng cách chèn thêm những đoạn lệnh rác không ảnh hưởng đến logic của chương trinfhxen kẽ giữa những mã lệnh thực sự.

**3) Các kỹ thuật của Virus máy tính trên mạng**

- Kỹ thuật lây nhiễm trên mạng:  
+ Sử dụng hàm GetLogicalDriveStrings để lây lan qua các ổ đĩa chia sẻ từ xa được ánh xạ thành ổ đĩa cục bộ.

+ Sử dụng các hàm API để liệt kê các ổ đĩa mà người dùng đã kết nối.

- Kỹ thuật phát tán virus trên mạng:

+ Chặn các hàm API hỗ trợ mạng.

- Kỹ thuật phá hoại trên mạng

+ Tạo các cổng nghe đợi sẵn để virus có thể tiến hành các hoạt động phá hoại hay do thám như lấy trộm mật khẩu, khởi động máy, phá hoại hệ thống…

+ Tấn công từ chối dịch vụ (DOS)

**4) Phòng chống virus máy tính:**

- Ý nghĩa:

+ Đảm bảo máy tính hoạt động ổn định.

+ Chống mất cắp các thông tin mật.

+ Bảo vệ dữ liệu an toàn.

- Cách phòng chống virus máy tính:

+ Hạn chế dùng đĩa mềm hoặc USB không rõ nguồn gốc mà chưa có sự kiểm tra bằng các phần mềm diệt virus.

+ Không cài đặt các phần mềm không cần thiết hoặc download từ trên mạng.

+ Không sử dụng các phần mềm không có bản quyền.

+ Không nên mở các thư điện tử lạ.

+ Cài các phần mềm chống virus tốt nhất.

+ Sao lưu dữ liệu thường xuyên.

- Các chương trình diệt Virus sẽ quét các tập tin thực thi, tập tin office, tập tin đính kèm E-mail, các tập tin được download và những dạng tập tin khác có thể trở thành host của Virus (Hostable files).

- Các phương pháp quét chuẩn bao gồm:

+ Basic scanning: tìm chữ ký của virus trong các tập hostable bao gồm cấu trúc, định dạng, các mẫu và những đặc trưng khác. Kiểm tra kích thước của các file hệ thống đã bị thay đổi để phát hiện nhiễm virus.

+ Heuristic scanning: quét các đoạn mã đáng ngờ trong các tập tin thực thi dựa trên công nghệ heuristics.

+ ICV scanning: sử dụng giải thuật HMAC để tính toán giá trị kiểm tra tính toàn vẹn của tập tin thực thi chưa bị nhiễm virus và 1 khóa mã hóa cố định. Một giá trị ICV được nối vào cuối của tập tin thực thi không bị nhiễm virus. Các virus không biết mật mã sẽ không thể thay đổi ICV. Khi 1 tập tin bị nhiễm virus, giá trị ICV của nó sẽ thay đổi so với giá trị ICV nguyên thủy.

* Các phần mềm độc hại

Malware (Phần mềm độc hại): Là một thuật ngữ tổng quát dùng để mô tả bất kỳ phần mềm có hành vi gây hại hoặc xâm phạm đối với máy tính hay hệ thống. Malware có thể bao gồm virus, worm, trojan, ransomware, spyware, adware và nhiều loại khác.

Virus:Là một chương trình máy tính có khả năng tự sao chép và gắn kết vào các tệp tin khác mà không cần sự sự chấp nhận hoặc sự hiểu biết của người sử dụng.

Worm (Sâu máy tính):Giống như virus, nhưng có khả năng tự lây lan qua mạng và các thiết bị khác mà không cần sự tương tác của người sử dụng.

Trojan (Trojan Horse):Là một loại malware được giấu giếm trong các tệp hoặc chương trình có vẻ hữu ích hoặc không nguy hiểm để lừa dối người sử dụng và tạo điều kiện cho việc tấn công từ bên trong.

Ransomware:Mã hóa dữ liệu trên máy tính của nạn nhân và đòi tiền chuộc để cung cấp khóa giải mã. Nếu người dùng không thanh toán, dữ liệu của họ có thể bị mất hoặc không thể truy cập.

Spyware:Thu thập thông tin về hành vi người sử dụng mà không sự chấp thuận của họ, thường được sử dụng để định hình quảng cáo hoặc thu thập thông tin cá nhân.

Adware:Hiển thị quảng cáo không mong muốn trên máy tính của người sử dụng, thường đi kèm với các ứng dụng miễn phí.

Keylogger (Ghi chú phím):Thu thập thông tin từ bàn phím của người sử dụng mà không họ biết, thường được sử dụng để đánh cắp thông tin đăng nhập và mật khẩu.

Rootkit:Là một loại phần mềm độc hại mà mục tiêu chính là ẩn đi sự tồn tại của nó hoặc sự tồn tại của các hoạt động độc hại khác trên hệ thống.

Botnet:Một mạng các máy tính bị nhiễm malware và được điều khiển từ xa để thực hiện các hành động xấu, như tấn công mạng hoặc gửi thư rác.