**ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC SÀI GÒN**

**LẠI TRẦN TRUNG KIÊN**

**VIRUS MÁY TÍNH TRONG GIAI ĐOẠN HIỆN NAY VÀ CÁCH PHÒNG CHỐNG**

**ĐỀ CƯƠNG ĐỒ ÁN CHUYÊN NGÀNH**

NGÀNH: CÔNG NGHỆ THÔNG TIN

**Hồ Chí Minh, năm 2023**

**ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC SÀI GÒN**

**LẠI TRẦN TRUNG KIÊN**

**VIRUS MÁY TÍNH TRONG GIAI ĐOẠN HIỆN NAY VÀ CÁCH PHÒNG CHỐNG**

**ĐỀ CƯƠNG ĐỒ ÁN CHUYÊN NGÀNH**

NGÀNH: CÔNG NGHỆ THÔNG TIN

**Giảng viên phụ trách**

**TS. PHAN TẤN QUỐC**

**Thành phố Hồ Chí Minh, năm 2023**

**1**

**MỞ ĐẦU**

1. **Lý do chọn đề tài.**
2. **Lịch sử nghiên cứu vấn đề.**
3. **Mục đích và nhiệm vụ nghiên cứu.**
4. **Đối tượng và phạm vi nghiên cứu.**
5. **Phương pháp nghiên cứu.**
6. **Giả thuyết khoa học.**
7. **Những đóng góp mới của đề tài.**
8. **Dự kiến nội dung của tiểu luận.**

Chương 1: Tổng quan về virus máy tính.

Chương 2: Biểu hiện và hình thức lây nhiễm.

Chương 3: Tác hại và cách phòng chống virus.

**Chương 1:Tổng quan về virus máy tính**

* 1. **Giới thiệu về virus máy tính.**

1.1.1.Virus máy tính và các tính chất.

1.1.2.Phân loại virus máy tính.

**1.2. BOOT VIRUS (B-virus).**

1.2.1.Phương pháp lây lan.

1.2.2.Phân loại Boot Virus.

1.2.3.Cấu trúc chương trình B-Virus.

**1.3. VIRUS TỆP (VIRUS FILE).**

1.3.1. Phương pháp lây lan.

1.3.2. Phân loại virus file.

1.3.3. Cấu trúc chương trình F-virus.

**2**

**1.4. VIRUS MACRO**

1.4.1. Định nghĩa

1.4.2. Cấu trúc trúc chương trình Macro-virus

**1.5. TROJAN.**

1.5.1. Định nghĩa TROJAN.

1.5.2. Phương pháp lây nhiễm của TROJAN.

1.5.3. Sự nguy hiểm của TROJAN.

1.5.4. Phân loại virus TROJAN.

1.5.5. Mục đích của TROJAN.

1.5.6. Phương thức hoạt động của TROJAN.

**1.6. INTERNET WORM**

1.6.1. Giới thiệu chung

1.6.2. Nguyên lý hoạt động

**Chương 2:Nhận dạng , phát hiện virus và phương thức hoạt của virus máy tính**

**2.1. Kỹ thuật nhận dạng virus**

2.1.1. Nhận dạng chính xác mẫu (Signature based delection).

2.1.2. Nhận dạng theo mã đại diện.

2.1.3. Scan theo string.

2.1.4. Nhận dạng hành vi đáng ngờ.

2.1.5. Kiểm soát liên tục.

2.1.6. Kết hợp các phương thức.

**2.2. Phương pháp phát hiện virus**

2.2.1. Quét (Scanner).

2.2.2. Checksum (Kiểm tra tổng).

2.2.3. Guard (Canh phòng)

3

**2.3. Phương thức hoạt động của virus máy tính.**

2.3.1. Qua các thiết bị lưu trữ di động.

2.3.2. Qua thư điện tử.

2.3.3. Qua mạng Internet.

**Chương 3:Tác hại và cách phòng chống virus**

**3.1. Tác hại.**

3.1.1. Tác hại.

3.1.2. Biến thể.

3.1.3. Khả năng vô hiệu hóa phần mềm diệt virus.

**3.2. Cách phòng chống virus.**

3.2.1. Sử dụng phần mềm diệt virus.

3.2.2. Tường lửa.

3.2.3. Cập nhật và sửa chữa các lỗi của hệ điều hành.

3.2.4. Vận dụng kinh nghiệm sử dụng máy tính của bản thân.

3.2.5. Bảo vệ dữ liệu máy tính.

**3.3. Dò tìm trong bộ nhớ**

3.3.1. Đối với B-Virus

3.3.2. Đối với RF-Virus

**3.4. Diệt virus và khôi phục dữ liệu**

3.4.1. B-Virus

3.4.2. F-Virus

3.4.3. Virus Trojan

3.4.4. Sâu Worm

**3.5. Tạo Virus máy tính**

**4**

**CHƯƠNG 1: TỔNG QUAN VỀ VIRUS MÁY TÍNH**

**1.1.Giới thiệu về virus máy tính**

**1.1.1. Virus máy tính và tính chất**

**1.1.1.1. Khái niệm**

**.**

Virus máy tính hay còn thường được mọi người gọi là vi rút là những đoạn mã chương trình do con người tạo ra ,được gắn vào các tệp tin để lây nhiễm . Chúng được thiết kế với mục đích nhằm xâm nhập vào máy tính người dùng từ đó lấy cắp các thông tin các nhân, xóa dữ liệu hay thậm chí là gửi email nặc danh và có thể tự nhân bản và sao chép chính nó vào các chương trình khác . Virus máy tính luôn tự động làm những việc mà chủ của nó lập trình sẵn, không cần đợi sự cho phép hay ra lệnh của người sử dụng . Các công việc của virus làm thường nhằm mục đích phá hoại sự hoạt động bình thường của máy tính, làm hỏng hoặc ăn cắp dữ liệu trên máy, hoặc đơn giản chỉ là những thông báo bất thường làm phiền người sử dụng .



**Virus máy tính với những đoạn mã chương trình được thiết kế với mục đích xâm nhập vào máy tính .**

**5**

Ban đầu, mục đích tạo ra virus để nhằm đáp ứng các công trình thử nghiệm nhưng càng về sau vì nhiều lí do trục lợi khác nhau mà virus đã trở nên nguy hiểm hơn khi chúng được sử dụng để hướng đến việc đánh cắp thông tin cá nhân người dùng, tạo cơ hội cho các tin tặc nắm quyền điều khiển hay những mục đích xấu xa khác . Hiện nay hệ điều hành Windows với số lượng người dùng đông đảo nên hiển nhiên đứng đầu trong danh sách hệ điều hành bị nhiễm virus nhiều nhất .

**1.1.1.2. Cấu trúc chung của virus máy tính**

- Thông thường, cấu trúc của một virus bao gồm 3 phần chính :

* Phần lây lan (infection): Cách hoặc những cách virus dùng để lây lan . Chức năng đầu tiên là tìm kiếm những đối tượng phù hợp, việc tìm kiếm có thể tích cực như trong trường hợp của virus lây file có thể tìm kiếm các file có kích thước và định dạng phù hợp để lây nhiễm, hoặc việc tìm kiếm cũng có thể bị động như trường hợp của virus macro . Khi đã tìm thấy đối tượng thích hợp lại có một số vấn đề được đặt ra, một vài virus cố gắng làm chậm việc lây lan lại bằng cách lây cho ít file hơn trong một lần để tránh việc bị phát hiện bởi người sử dụng, cũng có một vài virus lại chọn cơ chế lây nhiễm nhanh, hay nói cách khác lây càng nhanh càng tốt, càng nhiều càng tốt, nhưng tất cả các virus đều phải kiểm tra xem đối tượng đã bị lây nhiễm chưa (vì lây nhiễm nhiều lần lên cùng một đối tượng sẽ rất dễ bị phát hiện), ta có thể minh họa bằng một đoạn giả mã như sau :

BEGIN

IF ( tìm thấy đối tượng thích hợp )

AND ( đối tượng đó chưa bị lây nhiễm )

6

THEN ( lây nhiễm cho đối tượng )

END

Nếu đối tượng chưa bị lây nhiễm thì virus mới tiến hành cài đặt bản sao của nó vào đối tượng .

Đặc biệt sau khi lây nhiễm virus phải tiến hành xóa dấu vết để tránh việc bị phát hiện, ví dụ như phải trả lại ngày tháng tạo lập file gốc, trả lại các thuộc tính cũ cho file v...

* Phần thân (payload): Tất cả những gì virus thực hiện trên máy tính đã bị lây nhiễm (trừ phần lây lan). Đoạn giả mã sau mô tả cơ chế hoạt động của phần thân thông thường :

BEGIN

IF (đến thời điểm phá hoại)

THEN (kích hoạt)

END

Phần thân có thể thực hiện bất cứ điều gì, từ việc rất đơn giản như đưa ra một thông báo, vẽ một hình đồ họa nghịch ngợm tới việc định dạng lại ổ đĩa cứng hay gửi bản sao của mình qua email tới các địa chỉ trong số địa chỉ của nạn nhân .

* Phần điều kiện kích hoạt (trigger): Cơ chế kiểm tra điều kiện để thực hiện phần thân, có thể sau một số lần lây nhiễm nhất định, vào một ngày giờ nhất định hoặc thậm chí kích hoạt ngay ở lần thực thi đầu tiên (nhưng những virus như thế sẽ không thể lây lan được trong thực tế) . Một cơ chế kích hoạt có thể mô tả qua đoạn giả mã như sau :

BEGIN

IF ( thứ 6 ngày 13 )

7

THEN ( đã đến thời điểm phá hoại )

END

**1.1.1.3. Lịch sử phát triển của virus máy tính**

Về lịch sử hình thành virus máy tính, có một vài quan điểm khác nhau, dưới đây sẽ nêu tóm tắt và khái quát những điểm chung nhất nhằm làm rõ quá trình hình thành của virus máy tính :

* Thật ra cơ sở lý thuyết về virus máy tính đã xuất hiện từ rất lâu, năm 1949, John von Neumann (1903-1957) - một nhà toán học người Mỹ, gốc Hungary, đồng thời cũng là cha đẻ của kiến trúc máy tính số hiện đại - đã phát triển nền tảng lý thuyết tự nhân bản của chương trình máy tính. Ông đã viết bài về "Lý thuyết và cơ cấu của các phần tử tự hành phức tạp – Theory and Organization of Complicated Automata” trong đó nêu ra ý tưởng về các chương trình tự nhân bản . John von Neumann cho rằng chương trình máy tính có thể được tự động tái tạo. Đây chính là một trong những nền tảng lý thuyết mà sau này virus máy tính đã lợi dụng để phát tán và lây nhiễm .
* Cuối những năm 60, đầu thập niên 70, một chương trình máy tính với tên gọi là "Pervading Animal" đã xuất hiện trên các máy Univax 1108 với khả năng: tự nó có thể nối vào phần sau của các tập tin khả thi (lúc này vẫn chưa hình thành khái niệm virus máy tính).
* **Năm 1972 :** Veith Risak cho xuất bản bài báo “Tái tạo tự động với trao đổi thông tin tối thiểu”. Bài báo mô tả về một loại chương trình máy tính (với đầy đủ chức năng của virus như hiện nay) được viết bằng ngôn ngữ máy cho hệ thống máy tính SIEMENS 4004/35.

8

1. **Vào năm 1981 :** một vài chương trình máy tính (có chức năng như virus ngày nay) đầu tiên đã xuất hiện trong hệ điều hành của máy tính Apple II .
2. **Vào năm 1984 :** tại Đại học Nam California - Mỹ, Fred Cohen lần đầu tiên đưa ra khái niệm virus máy tính (computer virus) như ngày nay .
3. **Tới năm 1986 :** Virus "the Brain", là virus đầu tiên có khả năng ảnh hưởng tới máy tính cá nhân được tạo ra tại Pakistan bởi Basit và Amjad. Đoạn mã độc hại này được thiết kế ẩn trong phần khởi động (boot sector) của một đĩa mềm 360KB và nó có khả lây nhiễm tới tất cả các ổ đĩa mềm .
4. **Năm 1988 :** Virus Jerusalem tấn công đồng loạt vào máy tính của các trường đại học và các công ty thuộc nhiều quốc gia vào Thứ Sáu ngày 13. Đây là loại virus hoạt động theo đồng hồ của máy tính .
5. **Năm 1987 :** Virus đầu tiên tấn công vào tệp hệ thống command.com là virus có tên là "Lehigh". Virus này được phát hiện tại Đại học Lehigh, chúng tấn công các máy tính theo chuẩn IBM và tương thích chuẩn IBM .
6. **Vào 3/1988 :** Lần đầu tiên phần mềm phát hiện và chống virus được thiết kế để phát hiện và loại bỏ các virus Brain. Phần mềm này cũng chủng ngừa cho các đĩa mềm để chúng có thể an toàn trước virus Brain .
7. **Năm 1990 :** Chương trình tìm kiếm và diệt virus thương mại đầu tiên được giới thiệu bởi hãng Norton. Sau đó các hãng IBM,

9

McAfee cũng lần lượt giới thiệu các phần mềm diệt virus ra thị trường .

1. **Năm 1991 :** Virus đa hình (polymorphic virus) xuất hiện. Đầu tiên là virus có tên gọi "Tequilla". Loại virus này có khả năng tự thay đổi hình thức của nó, gây khó khăn cho các chương trình chống virus khi tìm diệt .
2. **Năm 1994 :** Một số người sử dụng do chưa có kinh nghiệm, và cũng vì lòng tốt nên đã chuyển tiếp cho nhau một thư điện tử cảnh báo tất cả mọi người không mở bất kỳ một thư điện tử nào có cụm từ "Good Times" trong dòng tiêu đề của thư .
3. **Năm 1995 :** Virus văn bản (macro virus) đầu tiên xuất hiện trong các đoạn mã macro của các tệp tin văn bản của phần mềm soạn thảo Microsoft Word và đã lan truyền nhanh qua rất nhiều máy tính. Loại virus này có thể làm hỏng hệ điều hành máy bị nhiễm, phá hủy các tệp văn bản .
4. **Năm 1999** : xuất hiện virus Tristate, có thể tấn công vào các tệp văn bản Word, các tệp bảng tính Excel và các tệp trình chiếu PowerPoint .
5. **Năm 2000 :** Virus Love Bug, còn có tên gọi khác là ILOVEYOU đã đánh vào tính hiếu kì của mọi người. Đây là một loại macro virus. Đặc điểm là nó dùng đuôi tập tin dạng "ILOVEYOU.txt.exe" .
6. **Năm 2003 :** Virus SQL Slammer, lan truyền với tốc độ kỉ lục, nó đã lây nhiễm vào khoảng 75 ngàn máy tính chỉ trong khoảng thời gian 10 phút .

**10**

1. **Năm 2004 :** Là năm đánh dấu một thế hệ mới của virus. Đó là virus worm Sasser. Loại virus có khả năng lây lan rất mạnh mẽ vì nó có thể tự động phát tán tới bất cứ máy tính nào kết nối mạng Internet mà không cần phải mở tệp đính kèm của thư điện tử, chỉ cần mở nội dung thư là nó đã có thể xâm nhập vào máy tính .

**Những cái tên virus máy tính cực kì nguy hiểm :**

1. **Morrís ( 1988 )**
2. **CIH ( 1988 )**
3. **Melissa ( 1999 )**

****

**Melissa ( 1999 )**

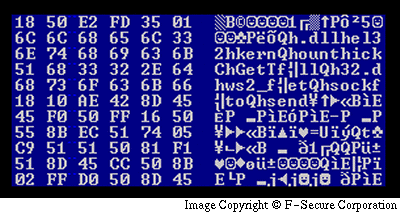
1. **ILOVEYOU ( 2000 )**

****

**ILOVEYOU ( 2000 )**

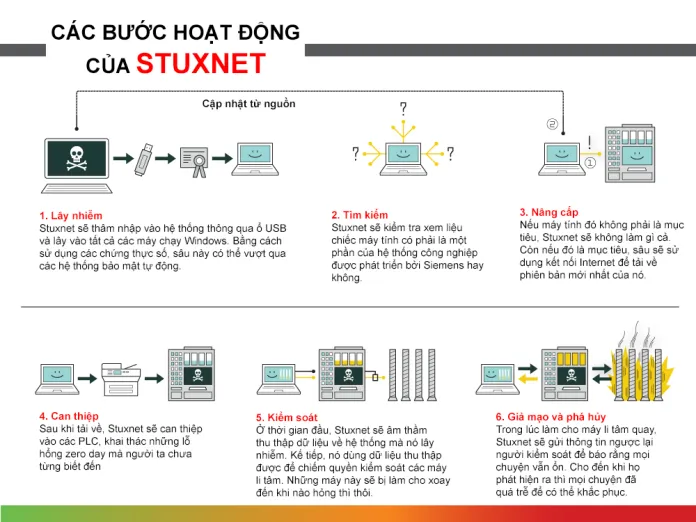
1. **Code Red ( 2001 )**
2. **SQL Slammer ( 2003 )**

**11**

****

**SQL Slammer ( 2003 )**

1. **Bagle ( 2004 )**
2. **MyDoom ( 2004 )**
3. **Zeus ( 2009 )**
4. **Siêu virus Stuxnet ( 2010 )**

****

**13**

**11. FlashBack ( 2011 )**

**12. CryptoLocker ( 2013 )**

**13. Wannacry ( 2017 )**

**1.1.2. Phân loại virus máy tính**

Virus máy tính thường được phân loại theo bản chất và hình thức của việc lây nhiễm. Thông thường, virus máy tính được phân loại như sau :

**Loại 1 : Virus Boot (B-virus)**

- Lây vào Boot Sector.

- Có tốc độ lây lan chậm.

- Nếu boot máy từ một đĩa mềm (USB, CD,..) nhiễm B-virus, bộ nhớ của máy sẽ bị khống chế, kế tiếp là boot record của đĩa cứng bị lây nhiễm.

**Loại 2 : Virus tệp (File virus – F Virus)**

Loại này thường lây nhiễm các file khả thi .EXE, .COM, .DLL, .BIN, .SYS.... Loại virus này hoạt động khi các file khả thi bị nhiễm virus được thi hành và ngay lập tức chúng sẽ tìm cách lây nhiễm hoặc tiến hành thường trú trong bộ nhớ và chờ cơ hội lây nhiễm sang các file khả thi khác.

**Loại 3 : Virus Mailer**

Virus loại này tìm kiếm trong các chương trình e-mail (như MS outlook), lấy ra danh sách địa chỉ e-mail được lưu trữ trong đó và nhân bản e-mail rồi gửi vào danh sách này .

**Loại 4 : Virus văn bản (Macro Virus)**

14

Tác giả của loại virus này đã sử dụng một ngôn ngữ lập trình macro đơn giản hoá, thường là VBA để sản xuất ra các virus này. Loại này thường tấn công vào các ứng dụng trong bộ Microsoft Office, phổ biến Word và Excel .

**Loại 5 : Virus đa hình (Polymorphic Virus)**

Sau khi phát tán đến một máy tính khác, loại virus này có khả năng thay đổi mã chương trình để tránh sự phát hiện của các chương trình chống virus, do đó nó còn được gọi là virus đột biến .

**Loại 6 : Virus bọc thép (Armored virus)**

Loại virus này được thiết kế để gây khó khăn cho việc phát hiện hay phân tích nó, chúng có khả năng tự bảo vệ mình trước các chương trình chống virus nên rất khó để có thể tiêu diệt được nó.. loại virus này có khả năng tự che dấu rất tốt trước các phần mềm chống virus bằng cách thay đổi kích thước của tệp tin hoặc thay đổi cấu trúc thư mục .

**Loại 7 : Virus tàng hình (Stealth virus)**

Là loại virus tàng hình có nghĩa là nó sử dụng phương pháp khác nhau để ẩn mình tránh bị phát hiện. Đôi khi chúng tự động loại bỏ khỏi bộ nhớ tạm thời để tránh sự phát hiện của phần mềm diệt virus. Khi phần mềm chống virus được khởi động để phát hiện virus, chúng sẽ ẩn nguồn cấp dữ liệu của virus tạo nên một hình ảnh tập tin và khu vực khởi động sạch sẽ.

**Loại 8 : Retrovirus**

**15**

Là một loại virus luôn tìm cách tấn công nhằm vô hiệu hóa các phần mềm chống virus chạy trên máy tính.

**Loại 9 : Virus nhiều đặc điểm (Multiple Characteristic Viruses)**

Loại virus này có những đặc trưng khác nhau của nhiều loại virus và chúng cũng có nhiều khả năng gây hại khác nhau đối với máy tính và dữ liệu.

**Loại 10 : Trojan**

- Không có tính chất lây lan.

- Lây vào chính hệ thống.

**Loại 11 : Backdoor**

- Là 1 loại trojan.

- Cho phép Hacker có thể kết nối từ xa với máy nạn nhân.

**Loại 12 : Adware**

- Phần mềm quảng cáo bất hợp pháp.

- Tự động hiện ra các trang web quảng cáo.

**Loại 13 : Spyware**

- Phần mềm gián điệp.

- Thu thập thông tin cá nhân của chủ nhân chiếc máy mà nó được cài vào.

**Loại 14 : Sâu máy tính (worm)**

16

- Có sức lây lan rộng, nhanh và phổ biến nhất hiện nay.

- Lan truyền qua hệ thống mạng.

**Loại 15 : Rootkit**

Kiểm soát hệ điều hành hoặc phần mềm chạy trên một thiết bị phần cứng nhất định.

* 1. **BOOT VIRUS (B-virus).**
     1. **Phương pháp lây lan**

**B-Virus thường lây lan phổ biến nhất bằng cách sử dụng phương tiện vật lý.**Đĩa mềm hoặc ổ USB bị nhiễm virus kết nối với máy tính sẽ truyền khi VBR của ổ đĩa được đọc, sau đó sửa đổi hoặc thay thế mã khởi động hiện có. Lần tiếp theo người dùng cố gắng khởi động máy tính để bàn của họ, vi-rút sẽ được tải và chạy ngay lập tức như một phần của bản ghi khởi động chính. Các tệp đính kèm email cũng có thể chứa mã vi-rút khởi động. Nếu được mở, các tệp đính kèm này sẽ lây nhiễm vào máy chủ và có thể chứa hướng dẫn gửi thêm các lô email tới danh sách liên hệ của người dùng. Những cải tiến trong kiến ​​trúc BIOS đã làm giảm sự lây lan của virus khởi động bằng cách đưa vào tùy chọn ngăn chặn bất kỳ sửa đổi nào đối với khu vực đầu tiên của ổ cứng máy tính.

Việc loại bỏ vi-rút khu vực khởi động có thể khó khăn vì nó có thể mã hóa khu vực khởi động. Trong nhiều trường hợp, người dùng thậm chí có thể không biết mình đã bị nhiễm vi-rút cho đến khi chạy chương trình bảo vệ chống vi-rút hoặc quét phần mềm độc hại. Do đó, điều quan trọng là người dùng phải dựa vào các chương trình bảo vệ chống vi-rút được cập nhật liên tục có sổ đăng ký lớn về vi-rút khởi động và dữ liệu cần thiết để loại bỏ chúng một cách an toàn. Nếu không thể loại bỏ vi-rút do mã hóa hoặc làm hỏng mã hiện có quá mức, ổ cứng có thể cần được định dạng lại để loại bỏ sự lây nhiễm.

17

* + 1. **Phân loại Boot Virus**

Việc cất giữ Boot sector được B-Virus giải quyết theo hai hướng:

**Hướng thứ nhất là** virus cất Boot sector cũ vào một vị trí xác định trên mọi đĩa và chấp nhận rủi ro có thể bị mất sector này do ghi đè, dù chỗ cất dấu này có khả năng bị ghi đè thấp nhất. Hướng giải quyết này đơn giản và do đó chương trình thường không lớn. Chỉ dùng một sector thay thế Boot sector cũ và do đó loại này được gọi là SB-Virus (Single Boot Virus).

**Hướng thứ hai là** virus có thể cất Boot sector này vào một vị trí an toàn trên đĩa tránh mọi mất mát có thể xảy ra. Vì kích thước vùng an toàn có thể định bất kỳ, nên virus thường chiếm trên nhiều sector và được chia làm hai phần: một phần trên Boot sector và một phần trên vùng an toàn. Vì đặc điểm như vậy, loại virus này được gọi là DB-Virus (Double Boot sector).

**1/ SB-Virus**

Do tính chấp nhận mất mát dữ liệu nên chương trình ngắn gọn chỉ chiếm một sector. Thông thường SB-Virus chọn những nơi mà khả năng ghi đè lên là ít nhất để cất Boot sector cũ.

Đối với đĩa mềm, các nơi thường chọn là:

- Những sector cuối cùng của Root Directory vì ít khi người dùng khai thác hết số entry của thư mục gốc.

- Những sector cuối cùng của đĩa vì khi phân phối liên cung cho một tập tin nào đó, DOS bắt đầu tìm liên cung trống từ đầu vùng dữ liệu căn cứ vào entry của nó trên FAT.

- Đối với đĩa cứng thì đơn giản hơn vì trên hầu hết các đĩa track 0 chỉ chứa Master Boot record trên một sector, còn lại các sector khác trên

18

track này là bỏ trống không dùng đến. Do đó, các SB-Virus và hầu hết các DB-Virus đều chọn những sector trống trên track này làm nơi ẩn náu.

**2/ DB-Virus**

- Đối với đa số các virus thì kích thước 512 byte (thông thường kích thước của một sector là 512 bytes) không phải là quá rộng rãi. Do đó họ đã giải quyết bằng cách thay thế Boot sector cũ bằng Boot sector giả. Boot sector giả này làm nhiệm vụ tải tiếp phần mã virus còn lại trên đĩa vào bộ nhớ rồi trao quyền điều khiển. Sau khi cài đặt xong phần này mới tải Boot sector thật vào bộ nhớ.

Phần mã virus còn lại có thể được nằm ở một trong những nơi :

- Đối với đĩa mềm: qua mặt DOS bằng cách dùng những liên cung còn trống.Những entry tương ứng với các liên cung này trên FAT sẽ bị đánh dấu là hỏng để cho DOS sẽ không sử dụng đến nữa. Phương pháp thứ hai ưu điểm hơn là vượt ra khỏi tầm kiểm soát của DOS bằng cách tạo thêm một track mới tiếp theo track cuối cùng mà DOS có thể quản lý (điều này chỉ áp dung với đĩa mềm). Tuy nhiên phương pháp này có nhược điểm là có một số loại ổ đĩa mềm không có khả năng quản lý, khi track mới được thêm sẽ gây lỗi khi virus tiến hành lây lan. Do vậy phương pháp thứ nhất vẫn được các virus sử dụng nhiều hơn.

- Đối với đĩa cứng: mã virus có thể được cất giữ tại những sector sau Master Boot record hoặc những sector cuối của Partition sau khi đã giảm kích thước của Partition đi hoặc giải quyết tương tự như trên đĩa mềm (sử dụng những liên cung còn trống và đánh dấu những liên cung này trong bảng FAT là hỏng để cho DOS không sử dụng nữa) .

- Nói chung cấu trúc chương trình SB-Virus hay DB-Virus là như nhau.

**19**

**1.2.3.Cấu trúc chương trình B-Virus.**

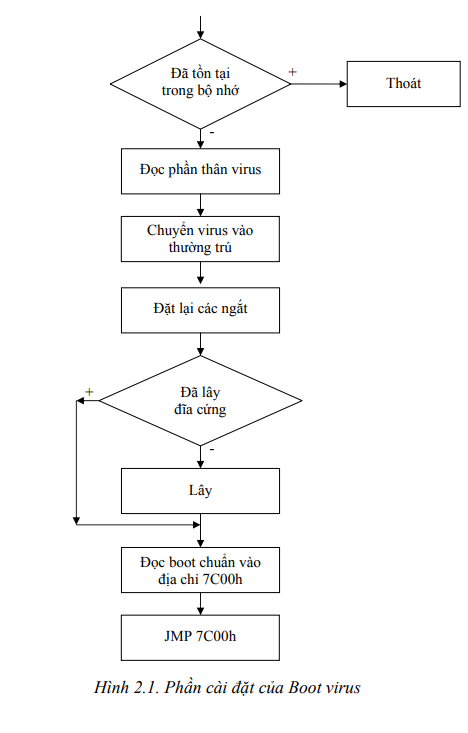
Do đặc điểm boot virus được thực hiện trước cả hệ điều hành nên nó có ưu thế là không bị phụ thuộc vào bất cứ hệ điều hành nào nhưng cũng có một nhược điểm là không sử dụng được các dịch vụ có sẵn của hệ điều hành mà phải tự thiết kế toàn bộ các thủ tục của mình.Vì chỉ được thực hiện một lần khi máy tính khởi động, thường boot virus phải thường trú trong bộ nhớ để có thể được xử lý nhiều lần, do đó chương trình boot virus được chia làm hai phần chính như sau :

**Phần cài đặt**

Là phần được thực hiện đầu tiên sau khi được trao quyền điều khiển từ đoạn mã nằm trong ROM. Chịu trách nhiệm tải phần thân vào bộ nhớ, thay thế các ngắt để đảm bảo giám sát liên tục được các hoạt động của hệ thống. Ta có thể mô tả hoạt động của phần cài đặt bằng lưu

đồ thuật toán sau :

20

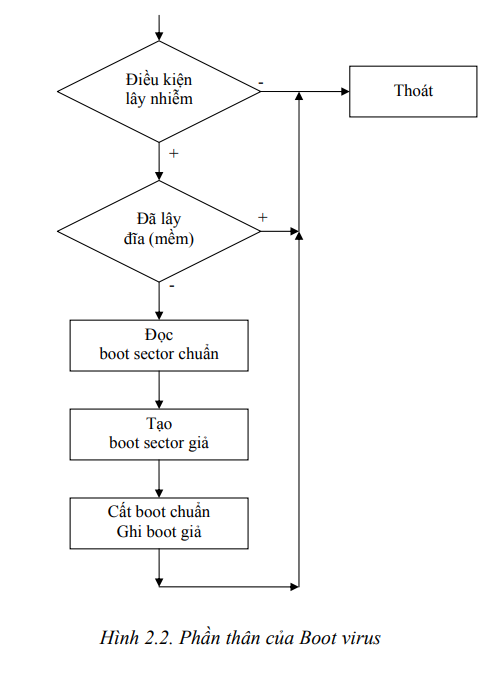


Dễ thấy chức năng đọc thân virus chỉ có ở DB virus vì với SB virus thì toàn bộ chương trình được đọc ngay khi nạp boot sector.

**Phần thân**

Thực hiện việc kiểm tra và lây lan trên các đối tượng thích hợp, phá hoại chương trình hoặc dữ liệu v.v..có thể mô tả bằng lưu đồ thuật toán như sau:

21



* 1. **VIRUS TỆP (VIRUS FILE)**
     1. **Phương pháp lây lan**

Virus lây nhiễm tập tin hệ điều hành có một khái niệm về tập tin được thực thi, trong một ý nghĩa rộng hơn các tập tin thực thi cũng có thể bao gồm các tập tin mà có thể chạy bởi các dòng lệnh người sử dụng như “shell”. Một tập tin lây nhiễm là một virus lây lan là những tập tin được hệ điều hành hay “shell” xem là để thực thi nó có thể bao gồm các tập tin

22

“batch” và mã kịch bản “shell” nhưng các mã nhị phân thực thi là những mã thực thi phổ biến nhất.

Để tiến hành lây nhiễm virus thực hiện ác công việc như sau:

• Tìm kiếm đối tượng tệp thực thi để lây nhiễm

• Nạp các mã độc lây nhiễm vào các tập tin tìm được

• Lưu trú và đảm bảo nó tồn tại duy nhất trong tập tin bị lây nhiễm

• Tiếp tục tìm kiếm các tệp tin khác để tiến hành lẫy nhiễm mã độc

Mỗi một loại virus sẽ có những cách thức để thực hiện lây nhiễm khác nhau song chúng đều được trải qua các nguyên lý bao gồm 3 giai đoạn là:

• Lây nhiễm và chiếm quyền điều khiển

• Chạy các chức năng của nó là các đoạn mã độc được gắn vào tệp tin lây nhiễm

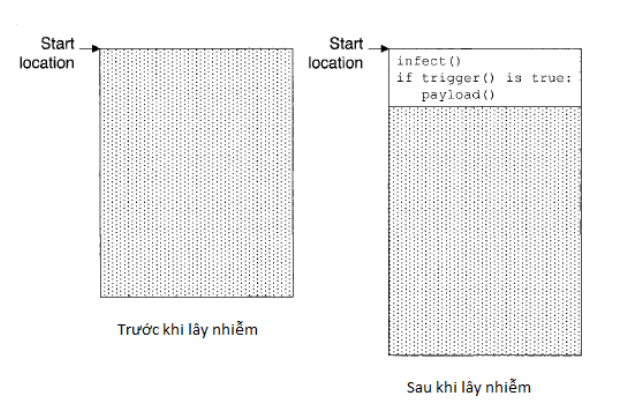
• Trao trả quyền điều khiển cho tệp và đảm bảo tính toàn vẹn ban đầu của dữ liệu.

Thông thường virus được tiến hành đặt ở hai nơi, nơi bắt đầu một tệp tin và nơi kết thúc hoặc một vị trí nào đó trong tệp tin, các kĩ thuật thực hiện của virus được trình bày như sau :

Lây nhiễm phần đầu của tập tin: các tập tin đơn giản thường có định dạng như .EXE, .COM, MS-DOS toàn bộ các tập tin được kết hợp bởi phần mã và phần dữ liệu. Khi được thực thi toàn bộ tập tin sẽ được nạp lên bộ nhớ và thực thi sẽ được bắt đầu bởi lệnh nhảy đến phần đầu

23

tiên nạp tập tin đó. Trong trường hợp này virus được đặt ở vị trí bắt đầu của tập tin nơi mà các tập tin nhận quyền điều khiển đầu tiên khi các tập tin bị lây nhiễm chạy nó sẽ thực thi các đoạn mã độc đầu tiên .

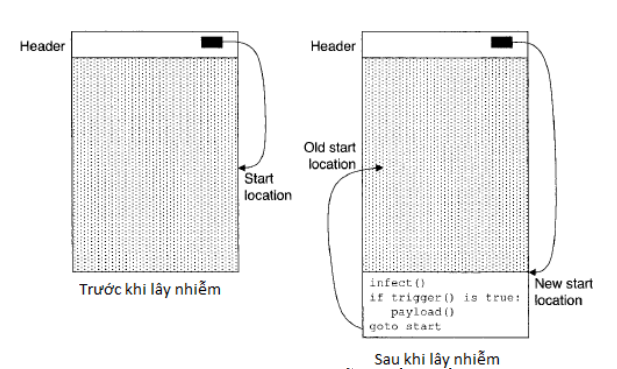


**Virus lây nhiễm phần đầu tệp tin**

Lây nhiễm phần cuối của tập tin: gắn thêm các mã vào phần cuối của một tập tin thì cực kì đơn giản, một virus đặt ở vị trí kết thúc một tập tin bằng cách nào nó có thể chiếm đoạt quyền điều khiển, có 2 phương pháp cơ bản như sau:

Các mã lệnh chương trình gốc có thể được lưu lại, và được thay thế bởi một lệnh nhảy đến các mã của virus, sau khi thực thi xong virus sẽ sử dụng quyền điều khiển trỏ đến các mã ban đầu mà nó đã lây nhiễm. Virus có thể sẽ cố gắng chạy trực tiếp các mã lệnh chương trình gốc ngay tại khu vực nó đã lưu hoặc virus có thể phục hồi các mã lệnh gốc này về trạng thái ban đầu và chạy nó.

24



**Virus lây nhiễm phần cuối tệp tin**

* + 1. **Phân loại virus file.**

Dễ thấy số lượng và cả chất lượng của các file virus vượt trội hơn hẳn các boot virus do chúng được chạy trên nền của hệ điều hành nên có thể tận dụng toàn bộ các ưu thế của hệ điều hành để thực hiện các ý đồ của mình. File virus được phân làm hai loại chính như sau :

**TF Virus (Transient File Virus) :**

Virus thuộc loại này không thường trú trong bộ nhớ, không chiếm các ngắt, khi được trao quyền nó sẽ tìm một hoặc nhiều file khác để lây lan.

**RF Virus (Residen File Virus) :**

Có thường trú trong bộ nhớ, khống chế hoạt động của máy tính bằng cách chiếm các ngắt (phổ biến nhất là ngắt 21h) để tiến hành lây lan.

* + 1. **Cấu trúc chương trình F-Virus**

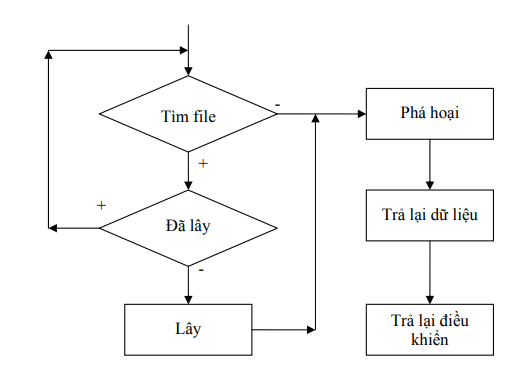
25

Do nguyên tắc hoạt động khác nhau nên cấu trúc của TF Virus và RF virus cũng khác nhau.

**TF Virus**

Vì nguyên lý làm việc đơn giản, không thường trú và không chiếm ngắt nên cấu trúc của một TF virus thường bao gồm ba phần chính:

**Phần lây lan**

Để đảm bảo sự tồn tại của mình, TF virus phải có phần lây lan càng mạnh càng tốt, tuy nhiên việc lây nhiều file cũng dẫn tới hậu quả là làm chậm tốc độ của hệ thống nên dễ bị phát hiện. Ta có thể mô tả hoạt động của phần lây lan bằng lưu đồ thuật toán sau :

Phần lây lan của File Virus

Để lây lan vào file đối tượng, thường file virus hay sử dụng một số phương pháp sau (chung cho cả hai loại RF virus và TF virus):

26

* Chèn đầu: Thường áp dụng để lây lên các file kiểu .COM do đặc điểm của file dạng này luôn có đầu vào cố định là 100h sau đầu đoạn do vùng 100h này được dành cho đoạn đầu chương trình (Program Segment Prefix – PSP). Virus sẽ chèn đoạn mã của mình vào đầu file đối tượng và đẩy đoạn mã của file này dịch đi một đoạn đúng bằng kích thước của virus. Ưu điểm là dễ thường trú trong bộ nhớ nhưng nếu kích thước file đối tượng lớn thì việc dịch chuyển file sẽ lâu, dễ bị phát hiện.
* Nối file: Virus sẽ nối đoạn mã của mình vào cuối chương trình đối tượng và phải định vị lại lệnh nhảy để chuyển điều khiển đến cho đoạn mã virus chứ không phải cho file đối tượng.
* Chèn giữa: Virus sẽ ghi đoạn mã của mình vào vùng trống trong file đối tượng (như stack). Ưu điểm của phương pháp này là không làm tăng kích thước chương trình lên nhiều, thậm chí không tăng nhưng lại hay gây ra lỗi nếu lạm dụng stack hoặc buffer của chương trình đối tượng.

**Phần phá hoại**

Không nhất thiết phải có, phương thức phá hoại cũng vô cùng đa dạng.

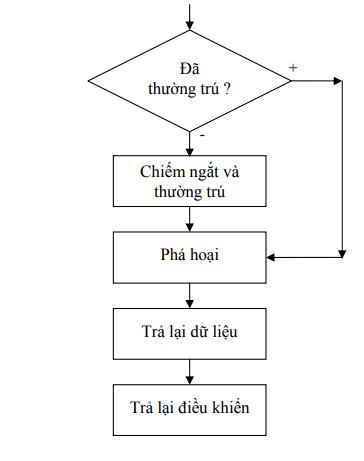
**Phần dữ liệu**

Chứa các dữ liệu nội tại của chương trình virus và các dữ liệu của chương trình đối tượng đang bị chiếm quyền.

**RF Virus**

27

Do phải giải quyết vấn đề thường trú và chiếm ngắt nên cấu trúc của RF Virus phải có thêm phần cài đặt, hoạt động của phần cài đặt có thể biểu diễn qua lưu đồ thuật toán như sau :



Phần cài đặt của RF Virus

**1.4. VIRUS MACRO**

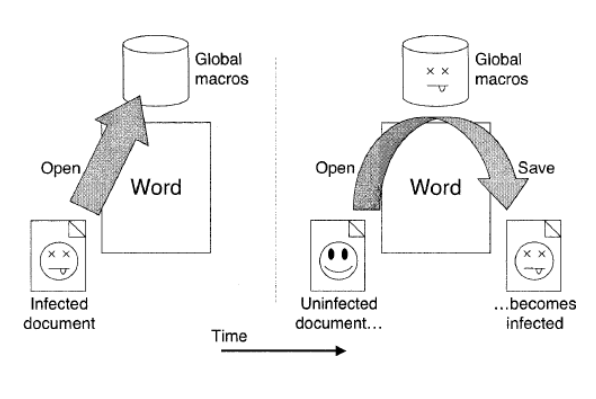
**1.4.1. Định nghĩa**

Năm 1995 cũng đánh dấu sự xuất hiện của macro virus, tuy đơn giản về kỹ thuật nhưng ý tưởng xây dựng nên dòng virus này lại cực kỳ thú vị, chỉ bằng cách khai thác những dòng mã lệnh và tính năng được thiết kế nhằm mang lại sự thuận tiện trong công việc của người sử dụng, những người viết virus có thể tạo nên các chương trình gây nên những tổn thất lớn về thời gian cũng như tiền bạc cho người sử dụng. Trong luận văn này chỉ đề cập đến các macro virus hoạt động trên chương trình

28

Microsoft Word và trong môi trường hệ điều hành Windows bởi lẽ nguyên tắc hoạt động của macro virus là gần giống nhau trên các chương trình ứng dụng khác nhau.

Một số ứng dụng cho phép chứa các tập tin dữ liệu, như các trình xử lý văn bản cho phép nhúng các hàm macro bên trong chúng, Macro là một đoạn mã nhỏ được viết bởi một ngôn ngữ chuẩn được biên dịch bởi ứng dụng, ngôn ngữ này cung cấp đầy đủ các hàm để viết một virus. Do vậy virus Macro chiếm được nhiều lợi thế hơn là virus lây nhiễm tập tin.



**Mô tả hoạt động của virus marco**

Khi một tài liệu chứa một macro được nạp bởi ứng dụng, macro có thể là lý do gây ra việc chạy tự động, cho phép kiểm soát điều khiển đến các virus macro. Một vài ứng dụng có thể tạo ra các cảnh báo người dùng về sự xuất hiện của marco trong văn bản tuy nhiên những cảnh báo này thường bị bỏ qua một cách dễ dàng. Trong hệ điều hành Windows thì Virus macro chủ yếu là các đoạn mã được viết bởi ngôn ngữ lập trình Visual Basic đây là một ngôn ngữ được sử dụng trong phần mềm thuộc bộ Microsoft Office như Word, PowerPoint, Excel.

Một tài liệu bị lây nhiễm thường bởi 2 kiểu macro với các tính chất:

**AutoOpen:** là các đoạn mã macro sẽ tự động chạy khi mà một tập tin được mở các macro này sẽ chiếm được quyền kiểm soát tập tin bị lây nhiễm.

**FileSaveAs:** là các đoạn mã lưu tập tin trong macro sẽ chạy khi mà tác vụ “File save as” trong trình đơn được lựa chọn. Nói cách khác đoạn mã này có thể được sử dụng để lây nhiễm đến bất kì tài liệu nào chưa bị nhiễm virus mà được lưu bởi người dùng.

Đứng trên quan điểm kỹ thuật, ngôn ngữ cho macro thì dễ dàng được sử dụng hơn các ngôn ngữ lập trình bậc thấp vì vậy lợi thế của macro làm giảm các rào cản tạo ra một virus.

**1.4.2. Cấu trúc trúc chương trình Macro-virus**

Về cấu trúc chương trình, macro virus cũng tuân theo các nguyên tắc cơ bản của virus máy tính, nghĩa là cũng có phần lây lan, phần dữ liệu, phần thân có thể có hoặc không tùy trường hợp.

Nguyên lý hoạt động của macro virus dựa trên việc bộ chương trình Office cho phép người sử dụng tự tạo ra các macro bằng ngôn ngữ lập trình dành cho các ứng dụng (Visual Basic for Application – VBA) để phục vụ cho công việc đặc thù của mình. Lợi dụng điều này, những

29

người viết virus tạo ra các macro có khả năng tự động thi khi chương trình ứng dụng khởi động hoặc tùy vào thao tác mà người sử dụng tác động vào hệ thống.

**1.5. TROJAN.**

**1.5.1. Định nghĩa TROJAN.**

Nhiều người nghĩ rằng khi họ có một chương trình quét virus tốt và có bản cập nhật mới nhất thì họ sẽ an toàn, máy họ sẽ không bị nhiễm. Trojan hay không ai có thể truy cập máy tính của mình, điều này hoàn toàn sai. Mục đích của người viết chương trình chống virus là phát hiện ra con virus mới, không phải là Trojan. Nhưng khi Trojan lây nhiễm đến nhiều người sử dụng thì những chuyên viên chống virus sẽ nạp thêm nó vào trong chương trình quét của mình. Tuy nhiên đây chỉ là một phần rất nhỏ các Trojan mà các chuyên viên phòng chống virus phát hiện được

và đưa vào trong danh sách những virus cần diệt.

Hơn nữa, các chương trình quét virus này không phải là tường lửa, nó sẽ không phát hiện ra trojan và bảo vệ ta trong khi ta đang trên mạng. Nhiều người dùng không biết Trojan là gì và họ tải xuống những file mà không biết rõ nguồn gốc.

**1.5.2. Phương pháp lây nhiễm của TROJAN.**

Theo số liệu thống kê của trung tâm BKIS 90% số người được hỏi có tải

xuống, hay sao chép file từ đâu đó không thì trả lời là không, nhưng thực sự họ đã thực hiện trước đó vài ngày.

Trojan có thể bị lây nhiễm từ rất nhiều con đường khác nhau:

- Trojan lây nhiễm từ ICQ

- Trojan lây nhiễm từ file đính kèm trong mail

- Trojan truy nhập trực tiếp

30

**Trojan lây nhiễm từ ICQ:**

Nhiều người nghĩ rằng Trojan không thể lây lan trong khi họ đang nói chuyện trên ICQ nhưng họ không nghĩ là người đang nói chuyện có thể gửi cho họ một con Trojan.

ICQ cho phép gửi một file .exe nhưng nó đã được sửa sao cho nhìn như có vẻ file đó là file hình ảnh, âm thanh…Ví dụ, có một con Trojan được kẹp chung với file hình ảnh và người gửi đã thay đổi biểu tượng của file .exe thành biểu tượng của file .bmp, người nhận sẽ chạy con Trojan đó và không hề nghi ngờ, vì khi chạy file .exe đó, nó vẫn hiện lên hình ảnh như một file ảnh. Kết quả là trên máy người nhận đã có một con Trojan. Đó là lý do hầu hết người dùng nói rằng họ không chạy bất kỳ file lạ nào trog khi họ đã chạy nó.

Một cách ngăn ngừa tốt nhất là luôn kiểm tra kiểu file trước khi chạy.

**Trojan lây nhiễm từ file đính kèm trong mail:**

Đa số Trojan được lây lan bằng mail. Các hacker hay chủ nhân của con Trojan thường đính kèm file Trojan vào trong một bức thư điện tử và gửi đi. Khi người dùng kích hoạt vào file đính kèm hay cả khi xem thư thì con Trojan đã có thể được kích hoạt xâm nhập hệ thống và thực hiện các chức năng đó.

**Trojan truy nhập trực tiếp:**

Một máy tính ngay cả khi được trang bị tốt nhất với những biện pháp bảo vệ, với chương trình chống virus tốt nhất thì cũng không thể làm gì được trước sự truy cập trực tiếp của người cố tình đưa Trojan vào trong máy tính.

**1.5.3. Sự nguy hiểm của Trojan**

Đa số mọi người cho rằng Trojan không có gì nguy hiểm, vì máy tính của họ vẫn làm việc bình thường và tất cả dữ liệu vẫn còn, nếu đó là một con virus thì dữ liệu đã có có thể mất sạch hay hoạt động không bình thường .

31

Khi máy tính bị nhiễm Trojan, tất cả dữ liệu trên máy tính có thể bị nguy hiểm, thường thì chủ nhân của Trojan này không xóa tất cả file, mà họ sẽ sao chép về khai thác như tài liệu bí mật của công ty, tài khoản Internet, tài khoản cá nhân và khi không có gì khác có thể thực hiện xóa dữ liệu. Đôi khi hacker còn dùng Trojan để cài đặt virus phá hoại như CIH chẳng hạn. Đó là một vài ví dụ hacker có thể thực hiện khi họ

đã cài thành công Trojan.

**1.5.4. Phân loại Trojan**

Có nhiều Trojan, nhưng chủ yếu nó được chia ra làm các dạng sau:

**Trojan dùng để truy cập từ xa :**

Hiện nay, Trojan này được sử dụng rất nhiều. Chức năng chính của Trojan này là mở một cổng trên máy tính nạn nhân để hacker có thể quay lại truy cập vào máy nạn nhân.

Trojan này rất dễ sử dụng. Chỉ cần nạn nhân bị nhiễm Trojan và chủ nhân của nó có địa chỉ IP của nạn nhân thì họ có thể truy cập toàn quyền trên máy nạn nhân.

Tùy loại Trojan mà chức năng của nó khác nhau (key logger, download, upload file, thực hiện lệnh..).

Một số con Trojan nổi tiếng loại này như: netbus, back orifice…

**Móc nối bàn phím (keylogger) :**

Nó ghi lại tất cả hành động trên bàn phím rồi lưu vào trong một file, hacker sẽ tìm đến máy tính đó và lấy đi file chứa toàn bộ thông tin về những gì người sử dụng đã gõ vào bàn phím.

Ví dụ: kuang keylogger, hooker, kuang2…

**Trojan gửi mật khẩu:**

Đọc tất cả mật khẩu lưu trong cache và thông tin về máy tính nạn nhân rồi gửi về đến hacker.

Ví dụ: barok, kuang, bario…

**Trojan phá hủy :**

32

Những con Trojan này chỉ có một nhiệm vụ duy nhất là tiêu diệt tất cả các file trên máy tính.

Ví dụ: CIH

Những con Trojan này rất nguy hiểm vì khi máy tính bị nhiễm chỉ một lần thôi thì tất cả dữ liệu mất hết.

**FTP Trojan:**

Loại Trojan này sẽ mở cổng 21 trên máy tính và để cho tất cả mọi người kết nối đến máy tính đó mà không cần có mật khẩu và họ sẽ toàn quyền tải bất kỳ dữ liệu nào xuống.

**1.5.5. Mục đích của Trojan**

Nhiều người nghĩ rằng hacker dùng Trojan chỉ để phá hoại máy của họ, điều đó hoàn toàn sai lầm. Trojan là một công cụ rất hữu hiệu giúp người sử dụng nó tìm được rất nhiều thông tin trên máy tính của nạn nhân.

- Thông tin về Credit Card, thông tin về khách hàng.

- Tìm kiếm thông tin về account và dữ liệu bí mật.

- Danh sách địa chỉ email, địa chỉ nhà riêng.

- Account Passwords hay tất cả những thông tin cơ vệ công ty.

**1.5.6. Phương thức hoạt động của TROJAN.**

Khi nạn nhân chạy file Trojan, nếu là Trojan dạng truy cập từ xa (remote

access), file server trong Trojan sẽ luôn ở chế độ lắng nghe. Nó sẽ chờ đến khi nhận được tín hiệu của Client, ngay lập tức nó sẽ mở ngay một cổng nào đó để hacker có thể truy cập vào. Nó có thể sử dụng giao thức TCP hoặc giao thức UDP.

Khi hacker kết nối vào địa chỉ IP của nạn nhân, họ có thể làm bất cứ điều gì vì nội dung Trojan đã bao hàm những điều khiển đó.

33

Còn nếu Trojan loại Keylogger hay loại gửi mật khẩu thì nó tiến hành việc ghi lại tất cả những gì được gõ trên bàn phím. Tất cả được lưu trữ trong một file theo một đường dẫn nhất định. Tại một thời điểm nào đó chủ nhân của con Trojan đó sẽ xâm nhập vào máy tính đó thông qua cổng sau mà con Trojan đã mở và lấy đi file đó. Đối với những con Trojan có phương thức gửi file trong bản thân nó thì nó tiến

hành gửi file đến địa chỉ email xác định trước.

Đối với Trojan loại phá hủy thì hoạt động của nó là nạp khi Windows khởi động và tiến hành công việc xóa file của nó.

Một vài Trojan được nạp ngay khi Windows được khởi động bằng cách sửa file win,.ini, system.ini hay sửa registry.

**1.6. INTERNET WORM**

1.6.1. Giới thiệu chung

Sâu máy tính là loại mã độc có khả năng tự nhân bản tuy nhiên chúng thường xuất hiện như những chương trình độc lập mà không cần tập tin chủ để mang nó. Do đó nó không ký sinh vào các tệp tin hoặc một khu vực nào trên đĩa cứng bản thân nó đã là một chương trình hoàn chỉnh vì vậy không thể dùng các chương trình dò quét tệp tin để phát hiện và loại bỏ sâu máy tính. Môi trường hoạt động của sâu máy tính là mạng Internet chúng đặc biệt mạnh trong khả năng tự nhân bản nếu như virus cần có một sự kiện từ người dùng để kích hoạt tự sao chép và lây nhiễm như là : Mở tập tin, khởi động máy tính, sao chép tập tin….Sâu máy tính hoàn toàn có khả năng sao chép và nhân bản chính nó mà không cần bất kỳ thao tác nào của người sử dụng đây là một đặc điểm giúp chúng lan rộng với tốc độ chóng mặt. Mục đích của sâu máy tính là làm tiêu tốn tài nguyên băng thông của mạng máy tính và phá hoại các hoạt động của hệ thống như là phá hủy tệp tin, tạo ra cửa hậu cho phép tin tặc xâm nhập và điều khiển trái phép hệ thống. Chính nhờ khả năng về tốc độ lan truyền và khả năng lẫy nhiễm xuyên các hệ thống trong khoảng thời gian ngắn làm cho các tin tặc ngày càng ưu thích sâu máy tính hơn là các virus thông thường, ngày nay mục tiêu thường thấy của sâu máy tính là thực hiện các cuộc tấn công từ chối dịch vụ Ddos hoặc thực hiện xâm nhập cài đặt các back door và tiến hành các công việc phá hoại vô cùng nguy hiểm.

Sâu máy tính bao gồm 2 loại chính là sâu dịch vụ mạng và sâu gửi điện thư hàng loạt.

**Sâu dịch vụ mạng (Network Service Worm):** chúng phát tán và lây lan thông qua việc khai thác các lỗ hổng bảo mật của các dịch vụ mạng, các ứng dụng hay hệ điều hành. Sau khi lây nhiễm vào hệ thống chúng sẽ dò quét tất cả các ứng dụng hay hệ thống chạy cùng dịch vụ với các lỗ hổng đang bị khai thác và tiếp tục tấn công trên diện rộng với tốc độ chóng mặt chúng có thể làm tê liệt mạng máy tính và các hệ thống an ninh, một số sâu dịch vụ mạng như là Sasser được phát hiện lây lan trên mạng ngày1/5/2004 bằng việc khai thác lỗ hổng bảo mật của dịch vụ LSASS (Local Security Authority Subsystem Service) tấn công vào các máy tính cài Windows 2000/ XP/ Server 2003. Hay một sâu dịch vụ nổi tiếng khác là Witty.

**Sâu gửi điện thư hàng loạt (Mass Mailing Worm):** Chúng là các sâu tấn công vào dịch vụ thư điện tử cách thức hoạt động của chúng là lây lan trên các hệ thống thư điện tử, một khi hệ thống bị lây nhiễm nó sẽ dò quét danh sách các địa chỉ email và tự động gửi bản sao của chính nó tới những địa chỉ mà nó tìm được bằng cách sử dụng các email máy khách thuộc hệ thống bị lây nhiễm hoặc email thuộc hệ thống do nó tạo ra, nó có thể gửi đồng loạt các thư này vào mạng lưới của hệ thống làm cho các máy chủ trở nên quá tải và làm cho hệ thống chịu một lượng lớn “bomb mail”. Loại sâu này hiện nay chủ yếu được dùng với mục đích quảng cáo như phát tán các thư rác hay những chương trình mã độc nguy hiểm khác một số ví dụ về sâu máy tính gửi điện thư hàng loạt là: Beagle, Mydoom và Netsky.

**1.6.2. Nguyên lý hoạt động**

Ta sẽ xem xét nguyên lý hoạt động của worm thông qua việc phân tích hoạt động của các worm cụ thể.

Melissa xuất hiện lần đầu tiên vào thứ 6 ngày 26 tháng 3 năm 1999, tại thời điểm đó nó được đánh giá là “lây lan nhanh nhất từ trước tới nay”. Nhiều tổ chức đã phải đóng hệ thống email của mình để tránh sự lây lan của virus.

Thực chất Melissa là một macro virus và lây lan trước hết trên các file văn bản của Microsoft Word 97/2000 nhưng điều đặc biệt là nó lại có tính năng lây lan rất mạnh qua mạng, sử dụng email như một công cụ để phát tán, dựa trên đặc điểm này ta sẽ xem xét hoạt động của nó như một worm. Xuất phát từ nhóm thảo luận có tên alt.sex trên Internet, macro của Melissa nằm trong file List.doc được hứa hẹn là chứa các password của các website xxx. Khi người sử dụng tải file này về và mở ra, macro AutoOpen sẽ tự động thực hiện.

Trước hết nó sẽ hạ mức bảo mật Macro Security của Microsoft Word xuống để cho phép chạy macro khi văn bản được mở ở những lần sau mà không có cảnh báo gì cho người sử dụng.

Khi macro được thi hành, nó sẽ tự đọng gửi email có đính kèm file list.doc tới 50 người nhận đầu tiên trong sổ địa chỉ (Address Book) của người sử dụng hiện tại. Email gửi đi thường có dạng sau:

**From:** (Tên của người sử dụng đã bị nhiễm worm)

**Subject:** Important Message From (Tên của người sử dụng)

**To:** (50 địa chỉ từ sổ địa chỉ) Here is that document you asked for ... don't show anyone else ;-) Attachment: LIST.DOC

Sau khi thực hiện lây lan qua email xong, Melissa tiếp tục lây nhiễm vào các file văn bản khác, điều nguy hiểm ở chỗ nó có thể gửi đi bất kỳ văn bản nào của người sử dụng chứ không cần là file list.doc như ban đầu, do đó dẫn đến nguy cơ người sử dụng sẽ bị lộ các thông tin nhạy cảm trong file khi nó được gửi ra ngoài.

Thủ tục phá hoại của Melissa chỉ đơn giản là chèn đoạn text dưới đây khi đến thời điểm ngày trùng với phút.

"Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here".

Toàn bộ hoạt động của worm Melissa có thể được mô tả qua hình dưới đây