TRƯỜNG ĐẠI HỌC SÀI GÒN
KHOA CÔNG NGHỆ THÔNG TIN

TIỂU LUẬN
HỌC PHẦN: HỆ ĐIỀU HÀNH

VIRUS MÁY TÍNH TRONG GIAI ĐOẠN HIỆN NAY VÀ BIỆN PHÁP PHÒNG CHỐNG

SVTH : TRẦN BÙI TY TY

GVHD: TS. PHAN TẤN QUỐC

Thành phố Hồ Chí Minh, tháng 11 năm 2023

TRƯỜNG ĐẠI HỌC SÀI GÒN
KHOA CÔNG NGHỆ THÔNG TIN

TIỂU LUẬN
HỌC PHẦN: HỆ ĐIỀU HÀNH

VIRUS MÁY TÍNH TRONG GIAI ĐOẠN HIỆN NAY VÀ BIỆN PHÁP PHÒNG CHỐNG

SVTH : TRẦN BÙI TY TY

GVHD: TS. PHAN TẤN QUỐC

Thành phố Hồ Chí Minh, tháng 11 năm 2023

LỜI CAM ĐOAN

Em xin cam đoan rằng bài tiểu luận *"Điện toán đám mây,vấn đề an toàn và bảo mật trong điện toán đám mây"* là kết quả của công việc nghiên cứu do bản thân thực hiện cùng với sự hỗ trợ từ giảng viên hướng dẫn thầy TS. Phan Tấn Quốc, bên cạnh đó là các tài liệu tham khảo, giáo trình liên quan đến đề tài nghiên cứu. Mọi thông tin, ý tưởng và nguồn tài liệu được sử dụng trong tiểu luận này đều được trích dẫn một cách chính xác và được viết lại dưới góc nhìn của bản thân.

Em xin chịu trách nhiệm về lời cam đoan của mình.

Trần Bùi Ty Ty

MỤC LỤC

DANH MỤC CHỮ VIẾT TẮT

Từ viết tắt	Tên tiếng Anh	Tên tiếng Việt
FAT sector	File Allocation Table sector	Bảng Phân Chia Tập Tin
USB	Universal Serial Bus	Cổng kết nối cáp
EPROM	Erasable Programmable Read-Only Memory	Bộ nhớ chỉ đọc có thể lập trình và xóa được
DNA	Deoxyribonucleic Acid	
RNA	Ribonucleic Acid	
PC	Personal Computer	Máy tính cá nhân
DOS	Disk Operating System	Hệ điều hành đĩa
VAX	Virtual Address eXtension	Hệ điều hành
VMS	Virtual Memory System	Hệ điều hành
ARPANET	Advanced Research Projects Agency Network	Mạng lưới cơ quan với các đề án nghiên cứu tân tiến
VBA	Visual Basic for Applications	Trực quan cơ bản cho các ứng dụng
DNS	Domain Name System	Hệ thống Tên miền
DDOS	Distributed Denial of Service	Tấn công phủ định dịch vụ phân tán
CD	Compact Disc	Đĩa nhỏ
IM	Instant Messaging	Trò chuyện tức thì
HTML	HyperText Markup Language	Ngôn ngữ đánh dấu siêu văn bản
ISP	Internet Service Provider	Nhà cung cấp Dịch vụ Internet

DANH MỤC HÌNH ẢNH

LỜI MỞ ĐẦU

Sự phát triển nhanh chóng của khoa học kĩ thuật và công nghệ đã đem lại rất nhiều lợi ích đối với cuộc sống hàng ngày của chúng ta. Các phần mềm và ứng dụng mới liên tục xuất hiện, mang lại sự tiện lợi và tối ưu hóa cho cách chúng ta làm việc, học tập và giải trí. Tuy nhiên, điều này cũng đồng nghĩa với sự gia tăng của mối đe dọa từ các loại phần mềm độc hại, đặc biệt là các virus máy tính. Chúng tấn công vào hệ thống máy tính và mạng, gây ra nhiều hậu quả nghiêm trọng cho người dùng cá nhân và doanh nghiệp. Tiểu luận này nhằm mục đích nghiên cứu sâu về các loại virus máy tính đang hoành hành trong thời đại hiện nay. Chúng tôi sẽ phân tích cách chúng hoạt động, cách chúng lây nhiễm và gây hại cho hệ thống máy tính. Ngoài ra, chúng tôi sẽ trình bày các biểu hiện cụ thể khi một máy tính bị nhiễm virus, giúp người dùng nhận biết và phản ứng kịp thời thông qua các nội dung chính:

Chương 1: Chúng tôi sẽ trình bày về khái niệm của Virus máy tính, đồng thời mô tả một số tính chât cơ bản của virus máy tính. Thảo luận về nguyên nhân xuất hiện và giới thiệu đến mọi người về thông tin và cấu tạo của virus máy tính hiện nay.

Chương 2: Ở chương này, chúng tôi sẽ tập trung mô tả và đánh giá sự lây lan thông qua các phương tiện khác nhau của virus máy tính. Sau đó giới thiệu một số biến biến thể mới của Virus máy tính và sự ảnh hưởng của chúng đến đời sống hiện nay.

Chương 3: Chúng tôi sẽ đề cập đến một số biểu hiện của máy tính khi bị nhiễm Virus máy tính, từ đó đưa ra một số giải pháp để giải viếc vấn đề đó. Bên cạnh đó chúng tôi sẽ thảo luận, gợi ý một số phần mềm diệt virus đề phòng chống và đề xuất cách bải vệ thông tin dữ liệu của máy tính khi bị nhiễm virus

CHƯƠNG 1: TỔNG QUAN VỀ VIRUS MÁY TÍNH

1.1 Sơ lược về Virus máy tính

Virus máy tính, từ khi xuất hiện cho đến nay, không ngừng khai thác các tiến bộ trong lĩnh vực công nghệ thông tin và truyền thông, cũng như lợi dụng những lỗ hổng nguy hiểm trong các hệ thống tin học để lan truyền những thông tin, những phần mềm độc hại vào máy tính người dùng, gây ảnh hưởng to lớn đến hệ thống an ninh mạng. Mặc dù việc sử dụng các thiết bị và phần mềm bảo mật trở nên phổ biến, nhưng virus vẫn tiếp tục phát triển mạnh mẽ. Hiện nay, chúng thường được tạo ra với mục đích cụ thể, phục vụ cho một đối tượng xác định, và liên tục được cải tiến qua các phiên bản để đạt được hiệu suất tốt nhất.

1.1.1 Khái niệm của Virus máy tính

Trong khoa học máy tính viễn thông, virus máy tính hay virus tin học (thường được người sử dụng gọi tắt là virus) là những đoạn mã chương trình được thiết kế để thực hiện tối thiểu là 2 việc:

- Tự xen vào hoạt động hiện hành của máy tính một cách hợp lệ, để thực hiện tự nhân bản và những công việc theo chủ ý của lập trình viên. Sau khi kết thúc thực thi mã virus thì điều khiển được trả cho trình đang thực thi mà máy không bị "treo", trừ trường hợp virus cố ý treo máy.
- Tự sao chép chính nó, tức tự nhân bản, một cách hợp lệ lây nhiễm vào những tập tin (file) hay các vùng xác định (boot, FAT sector) ở các thiết bị lưu trữ như đĩa cứng, đĩa mềm, thiết bị nhớ flash (phổ biến là USB)... thậm chí cả EPROM chính của máy.

Một virus máy tính có khả năng "nhiễm" các chương trình khác bằng cách sửa đổi chúng. Quá trình sửa đổi này bao gồm việc tiêm một đoạn mã

vào chương trình gốc, cho phép virus tạo ra các bản sao của chính nó và tiếp tục lây nhiễm sang các chương trình khác.[1]

Các virus sinh học là các đoạn mã di truyền siêu nhỏ, bao gồm DNA hoặc RNA, có khả năng chiếm quyền kiểm soát tế bào sống và gạt tế bào này vào việc sản xuất hàng ngàn bản sao hoàn hảo của virus gốc. Tương tự như phiên bản sinh học, virus máy tính cũng mang mã lệnh để tạo ra các bản sao hoàn hảo của chính nó. Một virus tiêu biểu sẽ bị nhúng vào một chương trình trên máy tính và sau đó, mỗi khi máy tính này chạy một chương trình chưa bị nhiễm, nó sẽ lây nhiễm vào chương trình mới đó. Do đó, nhiễm trùng có thể lan truyền từ máy tính này sang máy tính khác thông qua người dùng không hề hay biết, chẳng hạn khi họ trao đổi đĩa hoặc gửi các chương trình cho nhau qua mạng.[2] Trong môi trường mạng, khả năng truy cập các ứng dụng và dịch vụ hệ thống trên các máy tính khác cung cấp môi trường lý tưởng cho sự lan truyền của virus.

1.1.2 Bản chất và cấu trúc của virus máy tính

Bản chất của các virus là chúng có khả năng thực hiện mọi chức năng mà các chương trình khác có thể thực hiện. Sự khác biệt duy nhất là chúng kết nối và thực thi một cách bí mật khi chương trình chủ được chạy. Khi virus đang thực thi, nó có thể thực hiện bất kỳ chức năng nào được phép bởi quyền của người dùng hiện tại, chẳng hạn như xóa tệp và chương trình

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)
    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.v..[3]

• **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 sổ 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)

THEN (đã đến thời điểm phá hoại)

END[2]

1.1.3 Lịch sử hình thành

Có nhiều quan niệm khác nhau về lịch sử của virus điện toán. Ở đây chỉ nêu rất vắn tắt khái quát những điểm chung nhất, qua đó, chúng ta có thể hiểu chi tiết hơn về các loại virus:

Năm 1949: John von Neumann (1903-1957) phát triển nền tảng lý thuyết tự nhân bản của 1 chương trình cho máy tính.

Vào cuối thập niên 1960 đầu thập niên 1970 đã xuất hiện trên các máy Univax 1108 1 chương trình gọi là "Pervading Animal" tự nó có thể nối với phần sau của các tập tin tự hành, lúc đó chưa có khái niệm về virus.

Năm 1981: Các virus đầu tiên xuất hiện trong hệ điều hành của máy tính Apple II.

Năm 1983: Tại Đại học miền Nam California, tại Hoa Kỳ, Fred Cohen lần đầu đưa ra khái niệm "Virus máy tính" (computer virus) như định nghĩa ngày nay.

Năm 1986: Virus "the Brain", virus cho máy tính cá nhân (PC) đầu tiên, được tạo ra tại Pakistan bởi Basit và Amjad. Chương trình này nằm trong phần khởi động (boot sector) của 1 đĩa mềm 360Kb và nó sẽ lây nhiễm tất cả các ổ đĩa mềm. Đây là loại "stealth virus" đầu tiên. Cũng trong tháng 12 năm này, virus cho DOS được khám phá ra là virus "VirDem". Nó có khả năng tự

chép mã của mình vào các tệp tự thi hành (executable file) và phá hoại các máy tính VAX/VMS.

Năm 1987: Virus đầu tiên tấn công vào command.com là **virus "Lehigh".**

Năm 1988: Virus Jerusalem tấn công đồng loạt các đại học và các công ty trong các quốc gia vào ngày thứ Sáu 13. Đây là loại virus hoạt động theo đồng hồ của máy tính (giống bom nổ chậm cài hàng loạt cho cùng 1 thời điểm). Tháng 11 cùng năm, Robert Morris, 22 tuổi, chế ra **worm** chiếm cứ các máy tính của ARPANET, làm liệt khoảng 6.000 máy. Morris bị phạt tù 3 năm và 10.000 dollar. Mặc dù vậy anh ta khai rằng chế ra virus vì "chán đời" (boresome).

Năm 1990: Chương trình thương mại chống virus đầu tiên ra đời bởi Norton.

Năm 1991: Virus đa hình **(polymorphic virus)** ra đời đầu tiên là virus "Tequilla". Loại này biết tự thay đổi hình thức của nó, gây ra sự khó khăn cho các chương trình chống virus.

Năm 1994: Những người thiếu kinh nghiệm, vì lòng tốt đã chuyển cho nhau 1 điện thư cảnh báo tất cả mọi người không mở tất cả những điện thư có cụm từ "Good Times" trong dòng bị chú (subject line) của chúng. Đây là một loại virus giả **(hoax virus)** đầu tiên xuất hiện trên các điện thư và lợi dụng vào "tinh thần trách nhiệm" của các người nhận được điện thư này để tạo ra sự luân chuyển.

Năm 1995: Virus văn bản **(macro virus)** đầu tiên xuất hiện trong các mã macro trong các tệp của Word và lan truyền qua rất nhiều máy. Loại virus này có thể làm hư hệ điều hành. **Macro virus** là loại virus viết ra bằng công cụ VBA và tùy theo khả năng, có thể lan nhiễm trong các ứng dụng văn phòng của Microsoft như Word, Excel, PowerPoint, OutLook.... Loại macro này, nổi tiếng có **virus Baza** và **virus Laroux**, xuất hiện năm 1996, có thể

nằm trong cả Word hay Excel. Sau này, **virus Melissa**, năm 1997, tấn công hơn 1 triệu máy, lan truyền bởi 1 tệp đính kèm kiểu Word bằng cách đọc và gửi đến các địa chỉ của Outlook trong các máy đã bị nhiễm virus. **Virus Tristate**, năm 1999, có thể nằm trong các tệp Word, Excel và PowerPoint.

Năm 2000: Virus Love Bug, còn có tên **ILOVEYOU**, đánh lừa tính hiếu kì của mọi người. Đây là một loại macro virus. Đặc điểm là nó dùng đuôi tập tin dạng "ILOVEYOU.txt.exe", lợi dụng điểm yếu của Outlook thời bấy giờ: theo mặc định sẵn, đuôi dạng.exe sẽ tự động bị giấu đi. Ngoài ra, virus này còn có 1 đặc tính mới của spyware: nó tìm cách đọc tên và mã nhập của máy chủ và gửi về cho tay hắc đạo. Khi truy cứu ra thì đó là 1 sinh viên người Philippines. Tên này được tha bổng vì lúc đó Philippines chưa có luật trừng trị những người tạo ra virus cho máy tính.

Năm 2002: Tác giả của virus Melissa, David L. Smith, bị xử 20 tháng tù.

Năm 2003: Virus Slammer, một loại worm lan truyền với vận tốc kỉ lục, truyền cho khoảng 75.000 máy tính trong 10 phút.

Năm 2004: Đánh dấu 1 thế hệ mới của virus là **worm Sasser**. Với virus này thì người ta không cần phải mở đính kèm của điện thư mà chỉ cần mở lá thư là đủ cho nó xâm nhập vào máy. Cũng may là Sasser không hoàn toàn hủy hoại máy mà chỉ làm cho máy chủ trở nên chậm hơn và đôi khi nó làm máy tự khởi động trở lại. Tác giả của worm này cũng lập 1 kỉ lục khác: tay tin tặc nổi tiếng trẻ nhất, chỉ mới 18 tuổi, Sven Jaschan, người Đức. Tuy vậy, vì còn nhỏ tuổi, nên vào tháng 7/2005, tòa án Đức chỉ phạt anh này 3 năm tù treo và 30 giờ lao động công ích.

Năm 2017: Vụ tấn công của **WannaCry** vào ngày 12/5/2017 đang tiếp tục phát tán. WannaCry (tạm dịch là "Muốn khóc") còn được gọi là **WannaDecryptor 2.0**, là 1 phần mềm độc hại mã độc tống tiền tự lan truyền trên các máy tính sử dụng Microsoft Windows. Vào tháng 5/2017, 1 cuộc tấn

công không gian mạng quy mô lớn sử dụng nó được đưa ra, tính tới ngày 15/5 (3 ngày sau khi nó được biết đến) gây lây nhiễm trên 230.000 máy tính ở 150 quốc gia, yêu cầu thanh toán tiền chuộc từ 300 - 600 Euro bằng bitcoin với 20 ngôn ngữ (bao gồm tiếng Thái và tiếng Trung Quốc). Hiện thời người ta biết tới 5 tài khoản bitcoin của họ, đến nay chỉ có không hơn 130 người chịu trả tiền, thu nhập tối đa chỉ khoảng 30.000 Euro.[1]

Với khả năng của các tay tin tặc, virus ngày nay có thể xâm nhập bằng cách bẻ gãy các rào an toàn của hệ điều hành hay chui vào các chỗ hở của các phần mềm nhất là các chương trình thư điện tử, rồi từ đó lan tỏa khắp nơi theo các nối kết mạng hay qua thư điện tử. Do đó, việc truy tìm ra nguồn gốc phát tán virus sẽ càng khó hơn nhiều. Chính Microsoft, hãng phần mềm tạo ra các phần mềm phổ biến, cũng là 1 nạn nhân. Họ đã phải nghiên cứu, sửa chữa và phát hành rất nhiều các phần mềm nhằm sửa các khiếm khuyết của phần mềm cũng như phát hành các cập nhật của gói dịch vụ (service pack) nhằm giảm hay vô hiệu hóa các tấn công của virus. Nhưng dĩ nhiên với các phần mềm có hàng triệu dòng mã nguồn thì mong ước chúng hoàn hảo theo ý nghĩa của sự an toàn chỉ có trong lý thuyết. Đây cũng là cơ hội cho các nhà sản xuất các loại phần mềm bảo vệ, sửa lỗi phát triển.

Trong tương lai không xa, virus sẽ có thêm các bước biến đổi khác, nó bao gồm mọi điểm mạnh sẵn có (polymorphic, sasser hay tấn công bằng nhiều cách thức, nhiều kiểu) và còn kết hợp với các thủ đoạn khác của phần mềm gián điệp (spyware). Đồng thời nó có thể tấn công vào nhiều hệ điều hành khác nhau chứ không nhất thiết nhắm vào 1 hệ điều hành độc nhất như trong trường hợp của Windows hiện giờ. Và có lẽ virus sẽ không hề (thậm chí là không cần) thay đổi phương thức tấn công: lợi dụng điểm yếu của máy tính cũng như chương trình.[4]

1.1.4 Nguyên nhân xuất hiện

Các virus máy tính xuất hiện do một số nguyên nhân chính, bao gồm:

• **Lợi nhuận:** Một số người tạo ra các virus máy tính với mục tiêu kiếm tiền bất hợp pháp thông qua hoạt động phạm pháp như lừa đảo trực tuyến, ăn cắp thông tin cá nhân hoặc mã hóa dữ liệu của người dùng và đòi tiền chuộc. Việc này làm tăng sự xuất hiện của các virus máy tính với mục tiêu tài chính.

• **Sự phát triển của công nghệ:** Các virus máy tính thường được phát triển để tận dụng các lỗ hổng bảo mật trong hệ thống và phần mềm. Với sự phát triển không ngừng của công nghệ và phần mềm, các lỗ hổng bảo mật mới xuất hiện, tạo cơ hội cho các hacker và tạo ra nhu cầu cho việc phát triển các virus mới.

• **Sự cạnh tranh trong môi trường mạng:** Các hacker thường thi đua để tạo ra các phần mềm độc hại mới và tiến xa hơn trong việc xâm nhập vào hệ thống máy tính và mạng. Điều này có thể dẫn đến sự xuất hiện liên tục của các loại virus mới để thách thức và vượt qua các biện pháp bảo mật.

• **Khả năng ẩn danh:** Một số virus máy tính được thiết kế để hoạt động mà không để lại dấu vết hoặc để che giấu bản thân trong các tệp hợp pháp, điều này khiến cho việc phát hiện và loại bỏ chúng trở nên khó khăn.

• **Phát triển công cụ và phần mềm tấn công:** Các hacker sử dụng các công cụ và phần mềm tấn công tiên tiến để tạo ra và triển khai các virus máy tính. Sự phát triển của các công cụ này cũng góp phần làm tăng sự xuất hiện của các virus mới nhằm mục đích mang lại lợi ích cho cá nhân.[5]

1.2 Các Virus máy tính phổ biến hiện nay

Dưới sự phát triển của công nghệ số hiện nay, sự hoành hành và lớn mạnh của virus đang ngày càng phát triển. Dưới đây sẽ là một số loại virus máy tính đang hoạt động mạnh hiện nay.

1.2.1 Browser Virus Hijacker

Một phần mềm độc hại gọi là "browser hijacker," hay còn được gọi là "browser redirect virus," là một loại phần mềm độc hại ảnh hưởng đến cài đặt trình duyệt web của người dùng và gian lận để buộc trình duyệt chuyển hướng đến các trang web mà người dùng không có ý định truy cập. Thường thì các trang web mà một browser hijacker sẽ chuyển hướng người dùng đến là có hại. Mặc dù trải qua một browser hijacking không phải là tình huống lý tưởng, nhưng với các biện pháp an toàn thích hợp, người dùng có thể bảo vệ dữ liệu cá nhân của họ và ngăn chặn việc bị browser hijacking[6].

Cách thức hoạt động của Hijacker:

• Các phần mềm browser hijacker hoạt động bằng cách lây nhiễm vào các thiết bị thông qua phần mềm độc hại được tải xuống qua tệp đính kèm trong email, tệp bị nhiễm, hoặc khi người dùng truy cập một trang web nhiễm virus.

• Đôi khi, phần mềm độc hại này có thể kết nối với một tiện ích mở rộng của trình duyệt hoặc gói phần mềm khác. Phần mềm browser hijacker cũng có thể xâm nhập vào thiết bị thông qua các lây nhiễm từ phần mềm miễn phí, adware hoặc spyware.

• Trong hầu hết các trường hợp, người dùng không tải phần mềm browser hijacker một cách có chủ đích - phần mềm độc hại này thường được gói kèm với một tệp hoặc phần mềm khác. Sau khi người dùng cài đặt phần mềm browser hijacker mà họ không biết, phần mềm độc hại này lây nhiễm vào trình duyệt web của người dùng bằng cách sử dụng mã để thay đổi hoạt động của trình duyệt.

• Cách mà một phần mềm browser hijacker hoạt động phụ thuộc vào mục đích của cuộc tấn công. Nó có thể tấn công vào các cài đặt và chức năng khác nhau của trình duyệt web để đạt được các kết quả khác nhau. Mức độ

gây rối của phần mềm browser hijacker có thể đa dạng, từ các thay đổi nhỏ như thêm thanh công cụ mới đến các cuộc tấn công lớn hơn nhắm vào hệ thống tên miền (DNS) và chuyển hướng người dùng đến các trang web để đánh cắp tên người dùng và mật khẩu của họ[7].

1.2.2 Virus Web Scripting

Web Scripting Virus là phần mềm độc hại có khả năng vi phạm bảo mật trình duyệt web. Khi vi phạm bảo mật trình duyệt web, nó sẽ tiêm một số mã độc hại để chiếm quyền điều khiển trình duyệt web và thay đổi một số cài đặt.

Cách thức hoạt động của Virus Web Scripting:

• Loại phần mềm độc hại này lây lan giống như bất kỳ loại virus máy tính nào khác. Nó chủ yếu lây lan nhờ sự trợ giúp của các quảng cáo trang web bị nhiễm virus xuất hiện trên trang web. Nó cũng có khả năng gửi một số thư rác và cố gắng làm hỏng dữ liệu của người dùng. Mục tiêu chính của virus viết kịch bản web là các trang mạng xã hội. Khi virus này ảnh hưởng đến trình duyệt web, nó có thể làm cho thiết bị chạy chậm. Nó có thể trao quyền cho một số cuộc tấn công nguy hiểm như tấn công DDOS[8].

1.2.3 Virus Macro

Trong thuật ngữ máy tính , Virus macro là Virus được viết bằng ngôn ngữ macro : ngôn ngữ lập trình được nhúng bên trong ứng dụng phần mềm (ví dụ: trình xử lý văn bản và ứng dụng bảng tính). Một số ứng dụng, chẳng hạn như Microsoft Office , Excel , PowerPoint cho phép nhúng các chương trình macro vào tài liệu sao cho macro sẽ tự động chạy khi tài liệu được mở và điều này cung cấp một cơ chế riêng biệt để các hướng dẫn máy tính độc hại có thể lây lan. Đây là một lý do khiến việc mở các tệp đính kèm không mong muốn trong e-mail có thể nguy hiểm . Nhiều chương trình chống Virus

có thể phát hiện Virus macro; tuy nhiên, hành vi của virus macro vẫn có thể khó phát hiện.[8]

Cách thức hoạt động của Virus Macro:

• Khi một tệp chứa Virus macro được mở, vi-rút có thể lây nhiễm vào hệ thống. Khi được kích hoạt, nó sẽ bắt đầu tự nhúng vào các tài liệu và mẫu khác. Nó có thể làm hỏng các phần khác của hệ thống, tùy thuộc vào tài nguyên mà macro trong ứng dụng này có thể truy cập. Khi các tài liệu bị nhiễm được chia sẻ với người dùng và hệ thống khác, Virus sẽ lây lan. Virus macro đã được sử dụng như một phương pháp cài đặt phần mềm trên hệ thống mà không có sự đồng ý của người dùng, vì chúng có thể được sử dụng để tải xuống và cài đặt phần mềm từ internet thông qua việc sử dụng phím bấm tự động

• Vì vi-rút macro phụ thuộc vào ứng dụng chứ không phải hệ điều hành , nên nó có thể lây nhiễm vào máy tính chạy bất kỳ hệ điều hành nào mà ứng dụng mục tiêu đã được chuyển sang. Đặc biệt, vì Microsoft Word có sẵn trên máy tính Macintosh nên virus macro word có thể tấn công một số máy Mac ngoài nền tảng Windows.[9]

1.2.4 Virus đa phần (Multipartite Virus)

Một virus đa phần là một loại phần mềm độc hại hoạt động nhanh chóng tấn công đồng thời vào khu vực boot và các tệp thực thi của thiết bị. Vi-rút đa phần thường được coi là gây nhiều vấn đề hơn so với các vi-rút máy tính truyền thống do khả năng lan truyền đa dạng của chúng. Chúng được xem là có khả năng gây hại nhiều hơn so với các vi-rút khác. Vi-rút đa phần nhiễm bệnh cho hệ thống máy tính nhiều lần, vào các thời điểm khác nhau và để loại bỏ vi-rút, nó phải được loại bỏ hoàn toàn khỏi hệ thống. Nếu không làm như vậy, hệ thống có thể bị nhiễm vi-rút liên tiếp nếu không loại bỏ toàn bộ các phần của vi-rút.

Cách thức hoạt động của Multipartite Virus:

• Vi-rút đa phần lan truyền khi một máy tính bị nhiễm bệnh được khởi động, đặc điểm này được gọi là "boot infector," và nó đặc biệt là gây phiền toái vì nó nhắm vào các khu vực quan trọng của ổ cứng máy tính. Chúng cũng có thể lan truyền bằng cách gắn kết vào các tệp thực thi.

• Khi khu vực boot bị nhiễm bệnh, việc bật máy tính chỉ cần kích hoạt vi-rút khu vực boot vì nó bám vào ổ cứng chứa dữ liệu cần thiết để khởi động máy tính. Sau khi vi-rút đã được kích hoạt, các tải trọng phá hoại được khởi đầu trong các tệp chương trình.[10]

1.2.5 Virus lây qua file (File Infector Virus)

Một vi-rút nhiễm bệnh tệp tin là một loại phần mềm độc hại nhiễm bệnh các tệp thực thi với mục đích gây hại vĩnh viễn hoặc làm cho chúng không thể sử dụng được. Một vi-rút nhiễm bệnh tệp tin ghi đè mã hoặc chèn mã bị nhiễm vào tệp thực thi. Loại vi-rút này có thể nhiễm bệnh trên nhiều hệ điều hành, bao gồm Macintosh, Windows và Unix.[8]

Cách thức hoạt động của File Infector Virus:

• Loại vi-rút này có thể gắn vào đầu, giữa hoặc cuối của các tệp thực thi. Nó tạo ra bản sao của mã của mình và lan truyền vào các tệp khác trong hệ thống máy tính. Ví dụ, vi-rút Cleevix nhiễm bệnh tất cả các tệp thực thi cầm tay trong thư mục hệ thống. Khi tệp bị nhiễm bệnh được thực thi, nó gửi một thông báo cho người dùng để cảnh báo rằng các tệp của bạn bị nhiễm bệnh.

• Các phần mềm nhiễm bệnh tệp tin có thể sao chép mã của họ vào đầu hoặc cuối của tệp thực thi. Khi vi-rút chèn mã của mình vào cuối tệp nguồn, nó được gọi là vi-rút đặt ở đầu (prepending virus). Nếu mã vi-rút được chèn vào đầu của tệp nguồn, nó được gọi là vi-rút đặt ở cuối (appending virus).[8]

TÓM TẮT CHƯƠNG 1

Chương 1 của luận văn tập trung vào việc giới thiệu về virus máy tính, mang đến một cái nhìn toàn diện về chủ đề này. Chương giúp cho người dùng hiểu được định nghĩa cơ bản về virus máy tính, đặc điểm chính của Virus máy tính là khả năng tự nhân bản và lan truyền, thường gây hại cho hệ thống máy tính. Sau đó, nội dung chuyển sang phân tích cấu trúc và bản chất của virus máy tính, giúp độc giả hiểu rõ về cách chúng hoạt động và tác động đối với hệ thống. Chương đi sâu vào lịch sử hình thành của virus máy tính, đưa ra cái nhìn tổng quan về sự phát triển của chúng từ những ngày đầu cho đến hiện nay. Trong phần này, có thể được thảo luận về những sự kiện quan trọng và các loại virus nổi tiếng đã xuất hiện và tiếp tục với việc phân tích nguyên nhân dẫn đến sự xuất hiện và phát triển của virus máy tính, có thể liên quan đến sự phổ biến của công nghệ thông tin trong xã hội ngày nay.Trong phần thứ hai của chương, tập trung vào các loại virus máy tính phổ biến hiện nay. Các loại bao gồm Virus Hijacker, Virus Web Scripting, Virus Macro, Virus đa phần (Multipartite Virus) và Virus lây qua file (File Infector Virus). Mỗi loại được mô tả cụ thể về cách chúng hoạt động và tác động đối với hệ thống máy tính.

Tóm lại chương này đặt nền móng cho việc hiểu rõ về virus máy tính, từ khái niệm cơ bản đến các thực tế và loại virus phổ biến, tạo ra sự hiểu biết sâu sắc về một trong những thách thức lớn trong lĩnh vực an ninh thông tin ngày nay.

CHƯƠNG 2: SỰ LÂY LAN VÀ ẢNH HƯỞNG CỦA VIRUS

2.1. Khả năng lây lan của Virus

Khả năng lây nhiễm của virus máy tính là một khía cạnh quan trọng trong lĩnh vực an ninh máy tính. Virus máy tính là các chương trình độc hại được thiết kế để tự sao chép và lây nhiễm máy tính mục tiêu mà chúng tấn công thông qua nhiều hình thức khác nhau và xuất hiện khắp nơi trong lĩnh vực máy tính. Sau đây chúng tôi sẽ đưa ra một số thông tin về các hình thức lây lân mà chúng tôi tìm hiểu được.

2.1.1 Lây lan qua thiết bị

Cách cổ điển nhất của sự lây nhiễm, bành trướng của các loai virus máy tính là thông qua các thiết bị lưu trữ di động:

- Thông qua các thiết bị như USB, ổ cứng ngoài, và thẻ nhớ, các Virus máy tính sẽ tự động sao chép và lây nhiễm các phần mềm độc hại vào máy tính hoặc thiết bị được sử dụng.

Tuy nhiên, trước đây, đĩa mềm và đĩa CD thường là các phương tiện phát tán phổ biến nhất cho các chương trình độc hại. Ngày nay, khi sử dụng đĩa mềm đã giảm đi đáng kể, các phương thức lây nhiễm này đã dịch chuyển sang các ổ USB, ổ cứng di động hoặc các thiết bị giải trí kỹ thuật số.[1]

2.1.2 Lây lan qua Email

Trong thời kỳ thư điện tử (email) đã trở thành một phương tiện giao tiếp phổ biến trên toàn cầu, các virus đã điều chỉnh cách thức lây nhiễm của họ, chuyển từ các phương thức truyền thống sang lây nhiễm qua email.

Một khi virus đã xâm nhập vào máy tính của nạn nhân, chúng có khả năng tự động tìm và thu thập danh sách các địa chỉ email có sẵn trong máy. Sau đó, chúng tự động gửi email chứa virus đến danh sách này thông qua

hàng loạt (mass mail). Nếu các máy tính thuộc danh sách nhận thư mà không phát hiện được sự lây nhiễm, virus sẽ tiếp tục mở rộng và lây nhiễm tiếp theo. Nhờ cách này, số lượng nạn nhân có thể tăng nhanh, khiến cho trong thời gian ngắn, hàng triệu máy tính có thể bị lây nhiễm. Tình hình này có thể dẫn đến tê liệt nhiều tổ chức trên toàn thế giới trong thời gian ngắn.[1]

Khi các phần mềm quản lý thư điện tử và phần mềm diệt virus đã kết hợp lại với nhau để ngăn chặn sự lây nhiễm tự động và phát tán hàng loạt đến các địa chỉ trong danh bạ của máy nạn nhân, những kẻ phát tán virus đã chuyển sang việc tự gửi thư chứa virus từ những địa chỉ mà họ đã thu thập trước đó.

Phương thức lây nhiễm qua email bao gồm các hoạt động sau:

- **Lây nhiễm vào các file đính kèm theo thư điện tử (attached mail)**. Khi đó người dùng sẽ không bị nhiễm virus cho tới khi file đính kèm bị nhiễm virus được kích hoạt (do đặc điểm này các virus thường được "trá hình" bởi các tiêu đề hấp dẫn như sex, thể thao hay quảng cáo bán phần mềm với giá vô cùng rẻ).
- **Lây nhiễm do mở 1 liên kết trong thư điện tử**. Các liên kết trong thư điện tử có thể dẫn đến 1 trang web được cài sẵn virus, cách này thường khai thác các lỗ hổng của trình duyệt và hệ điều hành. một cách khác, liên kết dẫn tới việc thực thi 1 đoạn mã, và máy tính bị có thể bị lây nhiễm virus.
- **Lây nhiễm ngay khi mở để xem thư điện tử:** Cách này vô cùng nguy hiểm bởi chưa cần kích hoạt các file hoặc mở các liên kết, máy tính đã có thể bị lây nhiễm virus. Cách này thường khai thác các lỗi của hệ điều hành[1].

2.1.3 Lây lan qua Internet

- Theo sự phát triển rộng rãi của Internet trên thế giới mà hiện nay các hình thức lây nhiễm virus qua Internet trở thành các phương thức chính của virus

ngày nay. Có các hình thức lây nhiễm virus và phần mềm độc hại thông qua Internet như sau:

- **Lây nhiễm thông qua các file tài liệu, phần mềm:** Là cách lây nhiễm cổ điển, nhưng thay thế các hình thức truyền file theo cách cổ điển (đĩa mềm, đĩa USB...) bằng cách tải từ Internet, trao đổi, thông qua các phần mềm...
- **Lây nhiễm khi đang truy cập các trang web được cài đặt virus** (theo cách vô tình hoặc cố ý): Các trang web có thể có chứa các mã hiểm độc gây lây nhiễm virus và phần mềm độc hại vào máy tính của người sử dụng khi truy cập vào các trang web đó.
- **Lây nhiễm virus hoặc chiếm quyền điều khiển máy tính thông qua các lỗi bảo mật hệ điều hành, ứng dụng sẵn có trên hệ điều hành hoặc phần mềm của hãng thứ ba**: Điều này có thể khó tin đối với một số người sử dụng, tuy nhiên tin tặc có thể lợi dụng các lỗi bảo mật của hệ điều hành, phần mềm sẵn có trên hệ điều hành (ví dụ Windows Media Player) hoặc lỗi bảo mật của các phần mềm của hãng thứ ba (ví dụ Acrobat Reader) để lây nhiễm virus hoặc chiếm quyền kiểm soát máy tính nạn nhân khi mở các file liên kết với các phần mềm này[1].

2.2 Sự phát triển của Virus

Dưới sự phát triển của khoa học và kỹ thuật máy tính, các virus cũng đã và đang phát triển lớn mạnh hơn. Rất nhiều biến thể của Virus máy tính đã được tìm thấy và gây ra nhiều tác động đến đời sống và các thiết bị máy tính.

2.2.1 Các biến thể của Virus hiện nay

Các biến thể của virus là kết quả của việc sửa đổi mã nguồn với mục tiêu chính là tạo ra sự khó khăn trong việc phát hiện chúng bởi các phần mềm diệt virus hoặc thay đổi hành vi của virus. Một số virus có khả năng tự tạo ra

các biến thể khác nhau, gây ra khó khăn trong quá trình phát hiện và tiêu diệt chúng. Trong trường hợp khác, một số biến thể mới xuất hiện sau khi phần mềm diệt virus đã nhận dạng virus gốc. Tại đây, tác giả gốc hoặc các tin tặc khác, đã nắm vững về mã nguồn của virus, tiến hành viết lại, nâng cấp hoặc cải tiến chúng để virus tiếp tục hoạt động và lây nhiễm máy tính của nạn nhân[1].

Một số biến thể của virus máy tính:

• Ransonware:

Ransomware là một dạng virus được mã hóa, được coi là một trong những mô hình hiện đại của tội phạm mạng, đe dọa tính toàn vẹn của các hệ thống thông tin. Khi ransomware xâm nhập vào máy tính, nó sẽ mã hóa hoặc hạn chế truy cập vào dữ liệu trên ổ cứng. Để khôi phục lại quyền truy cập và dữ liệu của họ, nạn nhân phải thực hiện việc chuyển tiền vào tài khoản chỉ định bởi kẻ tấn công.

- Tuy nhiên, cần nhớ rằng việc trả tiền cho hacker không đảm bảo 100% khả năng khôi phục dữ liệu hoặc thông tin cá nhân của nạn nhân. Trong nhiều trường hợp, ngay cả khi tiền đã được chuyển đi, dữ liệu vẫn không thể được giải mã và trả về cho nạn nhân[5].

Điểm khác biệt so với các virus máy tính trước:

Yêu Cầu Chuộc Tiền: Ransomware là loại virus duy nhất yêu cầu tiền chuộc từ nạn nhân. Người tấn công muốn nạn nhân phải trả một khoản tiền hoặc số tiền tiền ảo như Bitcoin để có khả năng giải mã dữ liệu của họ. Điều này tạo ra một động cơ tài chính cho tấn công và làm cho nó trở thành một mô hình tội phạm mạng khác biệt.

Mã Hóa Dữ Liệu: Mục tiêu chính của ransomware là mã hóa dữ liệu trên máy tính của nạn nhân, làm cho dữ liệu trở nên không thể đọc được. Sau đó, nó cung cấp khóa giải mã sau khi nạn nhân đã trả tiền.

Thông Báo Rõ Ràng: Ransomware thường hiển thị một thông báo rõ ràng trên máy tính của nạn nhân yêu cầu tiền chuộc. Thông báo này thường chứa hướng dẫn cụ thể về cách trả tiền và giải mã dữ liệu.

Thời Hạn Chặt Chẽ: Ransomware thường đặt ra một hạn chế thời gian ngắn cho nạn nhân trả tiền chuộc. Nếu hạn chế thời gian này qua, thì số tiền có thể tăng lên hoặc dữ liệu có thể bị xóa.

Ghi Rõ Danh Tính Nạn Nhân: Ransomware thường ghi danh tính nạn nhân, đôi khi thậm chí công khai danh sách các máy tính đã bị nhiễm trên mạng.

Khó Để Theo Dõi: Việc sử dụng tiền ảo như Bitcoin để trả tiền chuộc làm cho việc theo dõi và truy tìm tội phạm trở nên khó khăn hơn, vì giao dịch tiền ảo không dễ dàng theo dõi.

• Virus Worm (Sâu máy tính)

Đặc điểm quan trọng nhất là sâu cũng tự sao chép, nhưng quá trình tự sao chép của một sâu khác biệt ở hai điểm.

Thứ nhất, sâu là độc lập và không phụ thuộc vào các mã nguồn thực thi khác.

Thứ hai, sâu lan truyền từ máy tính này sang máy tính khác qua mạng. Giống như virus, những con sâu đầu tiên ban đầu chỉ tồn tại trong trí tưởng tượng.

- Thuật ngữ "sâu" lần đầu tiên được sử dụng vào năm 1975 bởi John Brunner trong tiểu thuyết khoa học viễn tưởng của ông, The Shockwave Rider (Thú vị là ông đã sử dụng thuật ngữ "vims" trong cuốn sách đó nữa). Các thử nghiệm về sâu thực hiện tính toán phân tán (không có ý đồ gây hại) được thực hiện tại Xerox PARC vào khoảng năm 1980, nhưng đã có ví dụ trước đó. Một con sâu có tên Creeper đã tự sao chép qua mạng Arpanet vào thập kỷ 1970, và sau đó có một con sâu khác có tên Reaper theo đuổi và loại bỏ Creeper. Một sự kiện quan trọng đối với Internet diễn ra vào ngày 2 tháng 11 năm 1988, khi một

con sâu đã làm tê liệt Internet đang trong giai đoạn phát triển. Con sâu này hiện được gọi là con sâu Internet hoặc con sâu Morris theo tên của tác giả sáng tạo nó, Robert Morris, Jr. Vào thời điểm đó, Morris mới bắt đầu nghiên cứu tiến sĩ tại Đại học Cornell. Ông dự định con sâu của mình sẽ lan truyền chậm và không gây phiền toái, nhưng điều xảy ra lại hoàn toàn ngược lại. Morris sau đó bị kết án vì việc trái phép truy cập máy tính và chi phí để khắc phục hậu quả từ con sâu của ông. Ông bị phạt tiền và thụ động và thực hiện công việc cộng đồng.[6]

Điểm khác biệt so với các virus máy tính trước:

Ở mức trừu tượng này, không có sự phân biệt giữa một con sâu và một loại virus. Sự khác biệt thực sự nằm ở cách chúng lan truyền. Lan truyền bằng cách nhiễm vào mã nguồn khác thuộc lĩnh vực của một virus; tìm kiếm một cách tích cực các máy tính dễ bị tổn thương trên mạng tạo ra một con sâu. Con sâu có thể được gọi là xâm chiếm hoặc nhiễm trùng nạn nhân của nó; thuật ngữ sau sẽ được sử dụng ở đây. Một bản sao duy nhất của một con sâu sẽ được gọi là một trường hợp của con sâu, khi cần thiết để tránh sự mơ hồ.

Trong một số trường hợp, con sâu được phân loại dựa trên phương pháp chính mà chúng sử dụng cho việc truyền tải. Con sâu sử dụng tin nhắn tức thì (IM) để lan truyền được gọi là con sâu IM, và con sâu sử dụng email là con sâu email. Ví dụ, nhiều con sâu email đến dưới dạng tệp đính kèm trong email, người dùng bị lừa để chạy tệp đó. Khi chạy, con sâu thu thập địa chỉ email từ máy tính và gửi email cho chính nó đến các địa chỉ đó. Lừa người dùng để thực hiện điều gì đó là kỹ thuật xã hội, và đây là một cơ chế mà con sâu sử dụng để nhiễm trùng máy tính.

Cơ chế khác mà con sâu sử dụng để nhiễm trùng là các yếu điểm kỹ thuật. Người dùng không cần bị lừa để chạy tệp đính kèm email, nếu chỉ việc xem email đã cho phép mã nguồn của con sâu thực thi thông qua một lỗi đệm tràn. Người dùng không cần phải tham gia vào quá trình này, nếu con sâu lan

truyền bằng cách sử dụng lỗi đệm tràn giữa các quá trình máy chủ mạng chạy liên tục trên các máy tính khác nhau. Một con sâu cũng có thể khai thác các giao dịch hợp pháp hiện có. Ví dụ, xem xét một con sâu có khả năng theo dõi và thay đổi giao tiếp mạng, đặc biệt là nằm trên máy chủ mạng. Con sâu có thể đợi đến khi các chuyển giao hợp pháp của tệp thực thi - truyền tệp, sử dụng hệ thống tệp mạng - và hoặc thay thế chính nó vào chỗ của tệp thực thi được yêu cầu hoặc chèn chính nó vào tệp yêu cầu theo cách giống như một loại virus. Hầu hết các chi tiết về con sâu đã được đề cập ở các chương trước, như các yếu điểm kỹ thuật và yếu điểm của con người. Con sâu cũng có thể sử dụng các kỹ thuật giống như virus để cố gắng che giấu bản thân; con sâu có thể sử dụng mã hóa và có thể là oligomorphic, polymorphic hoặc metamorphic. Chương này do đó chỉ xem xét sự lan truyền làm cho con sâu khác biệt so với virus, bắt đầu bằng việc xem xét hai con sâu quan trọng trong lịch sử.

2.2.2 Khả năng phát triển của các biến thể

Khả năng phát triển của các biến thể virus là một khía cạnh quan trọng của tội phạm mạng và bảo mật máy tính. Dưới đây là một số cách mà các biến thể virus có thể phát triển và tiến hóa:

• **Mã nguồn thay đổi:** Các biến thể virus có thể thay đổi mã nguồn của họ để tránh bị phát hiện bởi phần mềm diệt virus. Điều này có thể bao gồm việc thay đổi cấu trúc mã hoặc các giá trị hằng số để tạo ra một phiên bản virus mới mà phần mềm diệt virus không nhận dạng.

• **Mã hóa:** Một số virus sử dụng mã hóa để che giấu chính họ. Chúng có thể mã hóa các phần của mã nguồn hoặc dữ liệu để làm cho việc phân tích và phát hiện trở nên khó khăn hơn.[1]

• **Cách lan truyền mới:** Virus có thể phát triển các cách mới để lan truyền. Điều này có thể bao gồm sử dụng các lỗ hổng bảo mật mới hoặc tận dụng các kỹ thuật xâm nhập khác.

• **Sự thay đổi trong hành vi:** Một số biến thể virus có khả năng thay đổi hành vi của mình. Chẳng hạn, một phiên bản virus có thể được cập nhật để thực hiện các tác vụ khác nhau hoặc để thay đổi cách nó tương tác với hệ thống máy tính.

• **Sử dụng kỹ thuật che giấu mới:**Virus có thể sử dụng các kỹ thuật che giấu mới để tránh sự phát hiện, bao gồm việc sử dụng mã nguồn ngắn gọn hơn, chèn chương trình trong các tệp hợp pháp hoặc sử dụng các kỹ thuật chống phân tích.

• **Tự tổng hợp và tạo biến thể**: Một số virus có khả năng tự tạo ra các biến thể mới của chính họ, làm cho việc phân tích trở nên phức tạp hơn.

• **Sự tiến hóa thông qua học máy:** Các tội phạm mạng có thể sử dụng học máy để phát triển virus thông minh hơn. Học máy cho phép virus học từ kết quả của các cuộc tấn công trước đó và điều chỉnh hành vi của chúng để tránh bị phát hiện.

• **Phát triển qua cộng đồng hacker:** Một số biến thể virus phát triển thông qua sự đóng góp của cộng đồng hacker hoặc tội phạm mạng, trong đó các tác giả chia sẻ kiến thức và công cụ để phát triển virus mới.

- Các biến thể virus không ngừng phát triển và thay đổi để thách thức các biện pháp bảo mật và phần mềm diệt virus. Điều này đặt ra một thách thức không ngừng cho cộng đồng bảo mật và yêu cầu sự cảnh giác và nỗ lực liên tục trong việc bảo vệ máy tính và dữ liệu khỏi các mối đe dọa này[1].

2.3 Tác động của virus đến đời sống con người và thiết bị người dùng

Virus máy tính có tácđộng dáng kể đến đời sông con con người cũng như thiết bị máy tính mà ta sử dụng hằng ngày. Dưới dây sẽ là một số ảnh hưởng của chúng đến từng yếu tố trong cuộc sống:

2.3.1 Tác động đến đời sống con người

Virus máy tính có thể có nhiều tác động tiêu cực đối với cuộc sống con người và xã hội. Dưới đây là một số ảnh hưởng chính của virus máy tính:

• **Mất dữ liệu quan trọng:** Một số loại virus có khả năng xóa hoặc mã hóa dữ liệu quan trọng trên máy tính của nạn nhân. Điều này có thể gây ra mất mát không thể khôi phục được của tài liệu, hình ảnh, video, và dữ liệu cá nhân quan trọng.

• **Thất thoát tài chính:** Ransomware và các loại virus khác có thể yêu cầu tiền chuộc để giải mã dữ liệu hoặc thả khóa máy tính. Người dùng có thể phải trả một số tiền lớn để lấy lại dữ liệu hoặc máy tính của họ, và thậm chí sau khi trả tiền, không phải lúc nào cũng đảm bảo lấy lại dữ liệu hoàn toàn.

• **Mất thời gian và năng suất:** Virus máy tính có thể làm chậm hoặc làm tê liệt máy tính, dẫn đến mất thời gian và năng suất. Sửa chữa máy tính bị nhiễm virus cũng đòi hỏi sự nỗ lực và thời gian đáng kể.

• **Xâm nhập vào quyền riêng tư:** Một số virus có khả năng thu thập thông tin cá nhân của nạn nhân, bao gồm mật khẩu, tài khoản ngân hàng, và thông tin cá nhân. Những thông tin này có thể được sử dụng cho mục đích gian lận hoặc xâm nhập vào quyền riêng tư của nạn nhân.

• **Sự lo lắng và căng thẳng:** Sự xuất hiện của virus máy tính và nguy cơ mất dữ liệu có thể gây ra sự lo lắng và căng thẳng cho người dùng máy tính. Họ phải lo lắng về việc bảo vệ máy tính và dữ liệu của họ, và có thể phải thực hiện các biện pháp bảo mật phức tạp.

• **Tác động vào tổ chức và doanh nghiệp:** Virus máy tính có thể gây ra thiệt hại lớn cho tổ chức và doanh nghiệp. Sự ngừng hoạt động của hệ thống máy tính và mất dữ liệu quan trọng có thể gây ra sự gián đoạn trong hoạt động kinh doanh và thiệt hại tài chính.

• **Lây lan hàng loạt:** Các loại virus có khả năng lây nhiễm hàng loạt có thể gây ra cuộc khủng hoảng bảo mật toàn cầu. Một loại virus có thể lan

truyền nhanh chóng và lây nhiễm hàng loạt, gây ra sự lo lắng trong cộng đồng toàn cầu.[4]

2.3.2 Tác động đến thiết bị máy tính

Một số virus có khả năng vô hiệu hoá hoặc can thiệp vào hệ điều hành làm tê liệt các phần mềm diệt virus. Sau hành động này chúng mới tiến hành lây nhiễm và tiếp tục phát tán. Một số khác lây nhiễm chính vào phần mềm diệt virus (tuy khó khăn hơn) hoặc ngăn cản sự cập nhật của các phần mềm diệt virus. Kể cả cài lại hệ điều hành máy tính và cài diệt sau đó nhưng đã quá trễ.

Các cách thức này không quá khó nếu như chúng nắm rõ được cơ chế hoạt động của các phần mềm diệt virus và được lây nhiễm hoặc phát tác trước khi hệ thống khởi động các phần mềm này. Chúng cũng có thể sửa đổi file host của hệ điều hành Windows để người sử dụng không thể truy cập vào các website và phần mềm diệt virus không thể liên lạc với server của mình để cập nhật.

Từ đó ta có thể rút ra được một số tác động của virus đến máy tính:

• **Mất dữ liệu:** Một số virus có khả năng xóa hoặc mã hóa dữ liệu trên thiết bị máy tính. Điều này có thể dẫn đến mất mát không thể khôi phục được của tài liệu quan trọng, hình ảnh, video, và dữ liệu cá nhân.

• **Sự chậm trễ và tê liệt:** Virus có thể làm cho thiết bị máy tính chậm hoặc tê liệt. Họ có thể chiếm dụng tài nguyên hệ thống, làm mất tài nguyên xử lý và bộ nhớ, gây ra hiện tượng treo máy hoặc sự khó khăn trong việc thực hiện các tác vụ cơ bản.

• **Lây nhiễm và lan truyền:** Virus có khả năng lây nhiễm sang các tệp và chương trình khác trên thiết bị máy tính. Điều này có thể làm cho toàn bộ hệ thống trở nên không ổn định và gây ra sự lây nhiễm nhanh chóng.

• **Khắc phục và sửa chữa:** Loại virus nhất định có thể gây khó khăn trong việc loại bỏ và sửa chữa. Một số virus thậm chí có thể tự bảo vệ và ngăn chặn quá trình loại bỏ của phần mềm diệt virus.

• **Tình trạng bảo mật yếu:** Các loại virus có thể tạo ra cửa sau (backdoors) trong hệ thống máy tính, cho phép tin tặc xâm nhập và kiểm soát thiết bị từ xa. Điều này có thể dẫn đến việc lấy cắp thông tin cá nhân hoặc thực hiện các hoạt động không đúng đắn.

• **Sự mất kiểm soát:** Một số virus có thể chuyển máy tính thành một botnet, tức là máy tính được kiểm soát từ xa và sử dụng để thực hiện các tác vụ bất hợp pháp, bao gồm cuộc tấn công mạng.

• **Thất thoát tài chính:** Ransomware là một loại virus có khả năng mã hóa dữ liệu và yêu cầu tiền chuộc để giải mã. Người dùng có thể phải trả tiền để lấy lại quyền truy cập vào dữ liệu của họ.

• **Sự lo lắng và căng thẳng:** Sự xuất hiện của virus có thể gây lo lắng và căng thẳng cho người dùng máy tính, đặc biệt khi họ không biết liệu họ đã bị nhiễm virus hay không và đối diện với nguy cơ mất dữ liệu hoặc tiền bạc.

• **Tổ hợp với lỗ hổng bảo mật:** Một số virus có thể khai thác các lỗ hổng bảo mật trên thiết bị máy tính để xâm nhập và lan truyền. Điều này có thể đặt nguy cơ bảo mật cho toàn bộ hệ thống mạng.[4]

TÓM TẮT CHƯƠNG 2

Chương 2 tập trung vào việc phân tích cách virus máy tính lan truyền và tác động đối với hệ thống thông tin. Bắt đầu bằng khả năng lây lan của virus, chương này đề cập đến cách chúng có thể tận dụng nhiều thiết bị, từ USB đến email và internet, để nhanh chóng và rộng rãi lây nhiễm. Phân đoạn này giúp độc giả hiểu rõ hơn về cơ chế truyền nhiễm của virus và cách chúng có thể vượt qua các rào cản an ninh.

Tiếp theo, chương đi sâu vào sự phát triển của virus, đưa ra cái nhìn về đa dạng của chúng thông qua giới thiệu về các biến thể phổ biến và khả năng phát triển độc lập của từng biến thể. Việc này nhấn mạnh tính động và linh hoạt của virus máy tính trong việc thích ứng với các biện pháp bảo mật mới.

Cuối cùng, chương tập trung vào tác động tiêu cực của virus đối với đời sống con người và thiết bị máy tính. Bằng cách phân tích các trường hợp, chương giải thích cách virus có thể gây mất dữ liệu quan trọng, đánh cắp thông tin cá nhân, và tạo ra tình trạng không an toàn trong cả môi trường trực tuyến và offline. Đồng thời, tác động của virus đối với thiết bị máy tính cũng được thảo luận, từ sự chậm trễ đến những hậu quả nặng nề như hỏng hóc và mất khả năng hoạt động. Tổng cảnh này giúp định rõ sự nguy hiểm và tính phổ biến của vấn đề này trong thế giới công nghệ hiện đại.

CHƯƠNG 3: PHÁP HIỆN BÀ BIỆN PHÁP PHÒNG CHỐNG

3.1 Biểu hiện của máy tính bị nhiễm Virus máy tính

Biểu hiện của máy tính bị nhiễm virus máy tính có thể biểu hiện qua nhiều dạng khác nhau. Máy tính nhiễm virus thường xuất hiện các dấu hiệu như chậm chạp trong quá trình hoạt động, giảm hiệu suất tổng thể, xuất hiện các cửa sổ pop-up không mong muốn và mất kiểm soát truy cập internet. Các biểu hiện khác có thể bao gồm mất dữ liệu quan trọng, thay đổi trang chủ trình duyệt, tăng sử dụng tài nguyên hệ thống, và thậm chí là việc gửi email hoặc tin nhắn không mong muốn đến danh bạ liên lạc của người dùng. Khi phát hiện bất kỳ dấu hiệu nào, người sử dụng cần ngay lập tức thực hiện các biện pháp diệt virus và khắc phục để ngăn chặn và loại bỏ virus từ hệ thống máy tính của mình.

3.1.1 Dấu hiệu đặc thù khi máy tính bị nhiễm Virus

Dấu hiệu của sự nhiễm virus máy tính có thể đa dạng và phụ thuộc vào loại virus cụ thể. Dưới đây là một số dấu hiệu đặc thù mà người dùng có thể chú ý:[10]

• Hiệu suất giảm:

Dấu hiệu của máy tính giảm hiệu suất có thể là một chỉ báo rõ ràng của việc máy tính bị nhiễm virus. Khi hiệu suất bắt đầu giảm, người dùng có thể gặp phải nhiều vấn đề khác nhau. Máy tính có thể khởi động chậm, mất nhiều thời gian hơn để mở các ứng dụng và trả lời các thao tác của người sử dụng. Trình duyệt web cũng có thể trở nên chậm chạp khi mở các trang web hoặc tập tin. Các ứng dụng có thể trở nên không phản hồi, và việc đóng chúng trở nên khó khăn hơn. Điều này cũng có thể làm ảnh hưởng đến khả năng xử lý các trò chơi hoặc ứng dụng đòi hỏi tài nguyên cao. hiệu suất giảm kéo dài và

không được cải thiện sau khi thực hiện các biện pháp bình thường như khởi động lại máy tính, đó có thể là dấu hiệu rõ ràng của sự nhiễm virus.

• Thay đổi trong dung lượng ổ đĩa

Dấu hiệu thay đổi đột ngột trong dung lượng ổ đĩa có thể là một biểu hiện rõ ràng của sự nhiễm virus trên máy tính. Khi máy tính bị nhiễm, virus thường sao chép và lưu trữ bản sao của chính nó trên ổ đĩa, làm tăng dung lượng lưu trữ mà không sự chấp thuận của người dùng do virus sao chép và lưu trữ bản sao của chính nó..

Dung lượng ổ đĩa giảm đột ngột có thể diễn ra nhanh chóng và đôi khi không thể lường trước được. Người dùng có thể phát hiện ra sự thay đổi này bằng cách kiểm tra dung lượng ổ đĩa trước và sau khi thấy máy tính bắt đầu hoạt động chậm hơn hoặc xuất hiện các dấu hiệu khác của sự nhiễm virus.[11]

• Cửa sổ pop-up và quảng cáo không mong muốn và trình duyệt web bị thay đổi không mong muốn

Dấu hiệu rõ ràng của sự nhiễm Virus trên máy tính có thể thể hiện qua xuất hiện đột ngột của cửa sổ pop-up và quảng cáo không mong muốn, cùng với các thay đổi không được phép trong trình duyệt web. Khi máy tính bị ảnh hưởng, người dùng thường xuyên phải đối mặt với sự phiền toái từ những cửa sổ pop-up xuất hiện mà không có sự tương tác từ phía họ. Những cửa sổ này thường chứa quảng cáo hay thông báo giả mạo, đôi khi có tính chất lừa dối để thu hút sự chú ý.

Ngoài ra, trình duyệt web có thể bị thay đổi mà không có sự cho phép từ người dùng. Trang chủ trình duyệt có thể bị thay đổi thành các trang web không mong muốn, và các tiện ích mở rộng hoặc công cụ tìm kiếm có thể được cài đặt một cách tự động mà không có sự đồng ý hay hiểu biết từ phía người sử dụng, đôi khi sẽ di chuyển đến các trang web độc hại, chứa các mã độc khác. Những thay đổi này không chỉ gây phiền toái mà còn có thể tạo ra

môi trường không an toàn, mở cửa cho rủi ro về an ninh mạng và bảo mật thông tin cá nhân.[12]

• Sự thay đổi trong hoạt động mạng

Người dùng cần chú ý đến một số biểu hiện quan trọng có thể xuất hiện khi máy tính của họ bị ảnh hưởng bởi virus hoặc malware. Một trong những dấu hiệu quan trọng là sự tăng đột ngột trong lưu lượng mạng. Khi lưu lượng mạng tăng lên mà không có nguyên nhân rõ ràng, đặc biệt là khi máy tính đang ở trạng thái không hoạt động, đây có thể là một tín hiệu cho thấy có hoạt động độc hại hoặc tấn công mạng đang diễn ra.

Ngoài ra các kết nối mạng không mong muốn là một dấu hiệu khác mà người dùng nên lưu ý. Virus có thể thay đổi cài đặt mạng để tạo ra kết nối không mong muốn, có thể được sử dụng để truyền tải thông tin đánh cắp hoặc thực hiện các hành động độc hại khác.

Tiếp đó là huyển hướng trình duyệt không đúng đắn, Virus có thể thay đổi cấu hình mạng để chuyển hướng trình duyệt sang các trang web độc hại mà người dùng không mong muốn, tăng nguy cơ rơi vào các kịch bản lừa đảo hay tấn công phishing.

Sự thay đổi trong cấu hình DNS cũng là một dấu hiệu quan trọng. Nếu máy tính gửi yêu cầu DNS đến máy chủ không an toàn, đây có thể dẫn đến việc kết nối đến các trang web giả mạo hoặc độc hại.

Cuối cùng, khả năng tham gia vào việc phát tán spam hoặc tấn công mạng. Máy tính bị nhiễm có thể trở thành một bộ phát tán spam hoặc tham gia vào các cuộc tấn công mạng, làm tăng lưu lượng mạng và tạo ra tình trạng không ổn định trên mạng.[13]

• Sự xuất hiện của các tập tin mới hoặc thay đổi trong các tập tin hiện có, hoặc mất dữ liệu, mã hoá tập tin

Một trong những biểu hiện đáng chú ý là xuất hiện các tập tin mới không rõ nguồn gốc, đặc biệt là những tập tin mà người dùng không nhớ tạo

ra. Nếu nội dung của các tập tin bị thay đổi mà không có sự tương tác từ phía người dùng. Bên ccajnh đó mất dữ liệu hoặc mã hoá tập tin là một biểu hiện nghiêm trọng, đặc biệt là khi người dùng phát hiện rằng các tập tin của họ đã bị mã hoá và yêu cầu thanh toán để khôi phục chúng. Đây thường là một chiến lược được sử dụng bởi Virus để gây thiệt hại và đe dọa người dùng. Ngoài ra còn có sự thay đổi trong phần mở rộng tập tin. Một số Virus có thể thay đổi phần mở rộng để ẩn đi sự thay đổi và làm cho người dùng khó nhận biết. Cuối cùng, sự mất mát dữ liệu đột ngột mà không có nguyên nhân rõ ràng cũng có thể là hậu quả của hoạt động độc hại[10].

• Sự xuất hiện của chương trình không mong muốn

Chương trình không mong muốn thường xuất hiện mà không có sự cho phép từ phía người dùng và thường đi kèm với mục đích thu thập thông tin cá nhân hoặc thực hiện các hành động độc hại khác. Các chương trình này có thể là adware, spyware, hoặc thậm chí là malware có thể gây ảnh hưởng nghiêm trọng đến hiệu suất và an ninh của hệ thống

• Thông báo bảo mật giả mạo

Thông báo giả mạo thường xuất hiện dưới dạng cửa sổ pop-up, trang web giả mạo, hay thậm chí là email nhắm vào người dùng. Chúng thường được thiết kế để giống như thông báo bảo mật chính thức từ các tổ chức đáng tin cậy như Microsoft, Apple, hay các công ty diệt virus nổi tiếng.

Nó thường chứa nội dung đe dọa, nhấn mạnh về sự cần thiết của việc người dùng phải thực hiện ngay lập tức. Các nội dung này có thể bao gồm việc báo cáo về việc máy tính bị nhiễm virus, dữ liệu cá nhân bị đe dọa, hay thậm chí là cảnh báo về việc tài khoản ngân hàng của họ có thể bị đóng.

Thông báo giả mạo đặt ra yêu cầu người dùng phải thực hiện một hành động ngay lập tức để giải quyết vấn đề, ví dụ như nhấp vào một liên kết, tải về một tập tin đính kèm, hay thậm chí là cung cấp thông tin tài khoản cá nhân. Chúng giả mạo giao diện người dùng được thiết kế để giống hệt các giao diện

thông báo bảo mật thực sự. Điều này có thể làm cho người dùng dễ bị lừa đảo, vì chúng có thể trông rất chính thức và đáng tin cậy[15].

Các thông báo giả mạo thường sử dụng logo, biểu tượng, và phông chữ giống như các tổ chức thực sự để tạo ra sự đánh lừa. Điều này giúp chúng tạo ra vẻ ngoại giao và đáng tin cậy.

3.1.2 Dấu hiệu không đồng nghĩa máy tính bị nhiễm Virus

Mặc dù nhiều dấu hiệu có thể là dấu hiệu của máy tính bị nhiễm virus, nhưng cũng có những tình trạng khác không phải do phần mềm độc hại. Dưới đây là một số dấu hiệu không phải lúc nào cũng chỉ ra rằng máy tính đã bị nhiễm virus:

• Phần Cứng Hoặc Phần Mềm Lỗi

Khi máy tính gặp vấn đề về phần cứng, người dùng thường có thể nhận diện những hiện tượng như hiệu suất kém, ứng dụng không đáp ứng, và thông báo lỗi thường xuyên. Dấu hiệu này có thể tương đồng với dấu hiệu ở phần trên nhưng nó vẫn có một số sự khác biệt đặc biệt, màn hình xanh (*Blue Screen of Death*) có thể xuất hiện, là một dấu hiệu của vấn đề nghiêm trọng trong hệ thống.

Ngoài ra, sự mất dữ liệu đột ngột, lưu trữ không thể truy cập được, âm thanh kém hoặc không hoạt động, cũng như các vấn đề liên quan đến màn hình hay đồ họa có thể là dấu hiệu của sự lỗi trong phần cứng máy tính. Các tiến trình không mong muốn chạy trong nền cũng có thể là một dạng hiện tượng liên quan đến vấn đề phần mềm.[10]

• Cập nhật hệ thống

Các vấn đề có thể xuất phát từ việc không cập nhật hệ điều hành, trình duyệt web, hoặc các ứng dụng khác lên phiên bản mới nhất. Thế nên sẽ có những trường hợp máy tính bị đơ, hiệu suất kém làm cho máy tính chậm hơn bình thường mất nhiều thời gian hơn để mở các ứng dụng và trả lời các thao

tác của người sử dụng. Các bản cập nhật thường cũng bao gồm các sửa lỗi liên quan đến bảo vệ dữ liệu. Ngoài ra nếu bạn không cập nhật, có thể tăng rủi ro mất mát hoặc thất thoát dữ liệu hoặc gặp pahri vấn đề tương thích khi sử dụng các ứng dụng mới.

• Sự Đầy Ổ Đĩa Cứng

Bên cạnh đó những sự biến đổi khác lạ của máy tính có thể xảy ra bởi việc đầy ổ nhớ .Sự đầy ổ đĩa cứng thường được phản ánh qua hiệu suất máy tính kém dẫn đến hoạt động không hiệu quả, khả năng lưu trữ giảm xuống, và thông báo lỗi về không gian lưu trữ. Nếu không đủ không gian, người dùng có thể gặp khó khăn khi cài đặt phần mềm mới hoặc lưu trữ dữ liệu.

• Thay Đổi Cấu Hình Người Dùng

Sự giống nhau giữa việc bị nhiễm virus và thay đổi cấu hình người dùng có thể tạo ra những dấu hiệu chung, mặc dù nguyên nhân có thể đa dạng. Một số sự đồng nhất có thể bao gồm thay đổi đột ngột trong trình duyệt web, như trang chủ bị thay đổi hoặc xuất hiện các cửa sổ pop-up quảng cáo không mong muốn. Điều này có thể là kết quả của cả sự can thiệp từ virus hoặc các ứng dụng không mong muốn có thể thay đổi cấu hình người dùng.

Ngoài ra, thay đổi trong cài đặt hệ thống như mở cổng mạng không mong muốn cũng có thể xuất hiện ở cả hai trường hợp. Quyền truy cập tệp và thư mục có thể bị thay đổi, làm cho người dùng không thể truy cập hoặc chỉnh sửa các tệp quan trọng. Tự động khởi động lại hoặc tắt máy tính cũng có thể là một dấu hiệu chung, có thể xuất phát từ sự can thiệp của virus hoặc do thay đổi không an toàn từ phía người dùng.[11]

• Quảng Cáo Trực Tuyến Thường Xuyên

Quảng cáo trực tuyến thường xuyên có thể là do các trang web truy cập thường xuyên nên dẫn tới việc nó xuất hiện mà người dùng không muốn. Ngoài ra còn là do Một số trang web có thể hiển thị quảng cáo trực tuyến thường xuyên để tăng doanh thu thông qua mô hình quảng cáo trả tiền.

3.1.3 Các đuôi tệp có khả năng bị nhiễm Virus

Các tập tin trên hệ điều hành Windows mang đuôi mở rộng sau có nhiều khả năng bị virus tấn công :

.bat: Microsoft Batch File (Tệp xử lý theo lô nhiều câu lệnh)

- .chm: Compressed HTML Help File (Tệp tài liệu dưới dạng nén HTML)
- .cmd: Command file for Windows NT (Tệp thực thi của Windows NT)
- .com: Command file (program) (Tệp thực thi)
- .cpl: Control Panel extension (Tệp của Control Panel)
- .doc: Microsoft Word (Tệp của chương trình Microsoft Word)
- .exe: Executable File (Tệp thực thi)
- .hlp: Help file (Tệp nội dung trợ giúp người dùng)
- .hta: HTML Application (Ứng dụng HTML)
- .js: JavaScript File (Tệp JavaScript)
- .jse: JavaScript Encoded Script File (Tệp mã hoá JavaScript)
- .lnk: Shortcut File (Tệp đường dẫn)
- .msi: Microsoft Installer File (Tệp cài đặt)
- .pif: Program Information File (Tệp thông tin chương trình)
- .reg: Registry File (Tệp can thiệp và chỉnh sửa Registry)
- .scr: Screen Saver (Portable Executable File)
- .sct: Windows Script Component
- .shb: Document Shortcut File
- .shs: Shell Scrap Object
- .vb: Visual Basic File
- .vbe: Visual Basic Encoded Script File
- .vbs: Visual Basic File (Tệp được lập trình bởi Visual Basic)
- .wsc: Windows Script Component
- .wsf: Windows Script File

• .wsh: Windows Script Host File
• .{*}: Class ID (CLSID) File Extensions[1]

3.2 Các biện pháp phòng chống Virus máy tính

Để đạt được mức độ bảo vệ tối đa trước nguy cơ lây nhiễm virus, có một số giải pháp triệt để mà người dùng có thể thực hiện. Tuy nhiên, cần lưu ý rằng trong thời đại ngày nay, việc không kết nối máy tính với "không gian số" là khó khăn, và một số biện pháp này có thể làm giảm trải nghiệm sử dụng. Dưới đây là một số biện pháp mạnh mẽ để hạn chế nguy cơ lây nhiễm virus:

3.2.1 Sử dụng phần mềm diệt Virus

Việc sử dụng phần mềm diệt virus là một phương tiện hiệu quả và thiết yếu trong việc bảo vệ máy tính và dữ liệu cá nhân khỏi các mối đe dọa trực tuyến ngày càng phức tạp. Với sự bùng nổ của công nghệ và mạng internet, mối đe dọa từ virus và các tác nhân độc hại khác ngày càng tăng cường và nguy hiểm hơn. Phần mềm diệt virus không chỉ giúp ngăn chặn sự xâm nhập của những mối đe dọa này mà còn cung cấp nhiều lợi ích khác.

Các ứng dụng diệt virus hiện đại không chỉ giúp phòng ngừa, phát hiện và loại bỏ các phần mềm độc hại, mà còn cung cấp khả năng quét hệ thống định kỳ và cập nhật định kỳ để đối phó với các mối đe dọa mới phát sinh. Chúng bảo vệ thông tin cá nhân, ngăn chặn email spam, và có thể ngay lập tức ngăn chặn các hành động độc hại trong thời gian thực.

Mặt khác, việc sử dụng phần mềm diệt virus cũng đôi khi gặp một số thách thức như tiêu tốn tài nguyên hệ thống hoặc khả năng phát hiện giả. Tuy nhiên, những ưu điểm này thường là nhỏ so với lợi ích lớn mà phần mềm diệt virus mang lại trong việc giữ cho máy tính an toàn và hiệu quả. Đặc biệt, với việc phát triển không ngừng của các mối đe dọa trực tuyến, việc sử dụng phần

mềm diệt virus trở thành một lựa chọn không thể thiếu để duy trì an toàn và bảo mật trong môi trường kết nối mạng ngày nay.[16]

Sau đây ột số lợi ích cũng như tác hại mà người dùng có thể gặp phải khi sử dụng phần mềm diệt Virus:

• Lợi ích

Phòng Ngừa Mối Đe Dọa: Phần mềm diệt virus giúp ngăn chặn xâm nhập của virus, malware và phần mềm độc hại khác vào hệ thống máy tính. Chúng tạo ra một lớp bảo vệ mạnh mẽ để ngăn chặn các mối đe dọa tiềm ẩn từ việc tấn công máy tính.

Quét Hệ Thống Định Kỳ: Tính năng quét hệ thống định kỳ của phần mềm diệt virus giúp phát hiện và loại bỏ các phần mềm độc hại mà người dùng có thể không nhận ra. Điều này giúp duy trì sự an toàn và ổn định cho máy tính.

Cập Nhật Định Kỳ: Việc cập nhật định kỳ về cơ sở dữ liệu mối đe dọa là chìa khóa để chống lại những mối đe dọa mới phát sinh đồng thời nhận biết và ngăn chặn các biến thể mới của virus.

Bảo Vệ Trực Tiếp: Nhiều phần mềm diệt virus hiện đại cung cấp bảo vệ trực tiếp trong thời gian thực, ngăn chặn các tệp độc hại từ việc thực hiện hành động trước khi chúng có thể gây hại cho hệ thống.

Phát Hiện Spam và Phishing: Ngoài việc ngăn chặn virus, phần mềm diệt virus cũng có khả năng phát hiện và ngăn chặn email spam và các trang web lừa đảo, bảo vệ người dùng khỏi những chiêu trò lừa đảo trực tuyến.

Hiệu Suất Máy Tính: Phần mềm diệt virus được thiết kế để hoạt động ẩn danh và không ảnh hưởng đến hiệu suất của máy tính. Điều này đảm bảo rằng bảo vệ máy tính không làm giảm tốc độ làm việc của người dùng.

Bảo Vệ Dữ Liệu Cá Nhân: Một trong những lợi ích quan trọng nhất là khả năng bảo vệ thông tin cá nhân và dữ liệu quan trọng của người dùng khỏi sự xâm nhập của virus.[1]

• Tác hại

Tiêu tốn tài nguyên hệ thống: Một số phần mềm diệt virus có thể tiêu tốn một lượng đáng kể tài nguyên hệ thống, đặc biệt là khi chúng đang thực hiện quét hệ thống. Điều này có thể dẫn đến giảm hiệu suất và làm chậm máy tính.

Có thể gây xung đột: Đôi khi, phần mềm diệt virus có thể gây xung đột với các ứng dụng khác hoặc thậm chí với hệ điều hành. Điều này có thể dẫn đến sự không ổn định hoặc giảm hiệu suất của hệ thống.

Phát hiện giả: Có trường hợp phần mềm diệt virus nhận diện một tệp tin là độc hại mà thực tế không phải là như vậy. Điều này có thể dẫn đến việc xóa nhầm các tệp tin quan trọng của người dùng.

Chi phí: Một số phần mềm diệt virus chất lượng cao có thể yêu cầu chi trả một khoản phí hàng năm hoặc hàng tháng. Điều này có thể là một gánh nặng tài chính đối với một số người dùng.

Khả năng bị vượt mặt: Mặc dù phần mềm diệt virus có hiệu suất cao, nhưng không thể đảm bảo hoàn toàn rằng nó sẽ ngăn chặn mọi mối đe dọa. Các hacker liên tục phát triển các kỹ thuật mới để bypass các biện pháp bảo vệ.

Ảnh hưởng đến kết nối internet: Một số phần mềm diệt virus có thể làm chậm kết nối internet của người dùng do việc quét và phân tích dữ liệu truyền qua mạng.

Khả năng gây loại bỏ ứng dụng hữu ích: Trong một số trường hợp, phần mềm diệt virus có thể nhầm lẫn và xem xét các ứng dụng hữu ích là độc hại, dẫn đến việc xóa chúng mà không cần thiết.

Nguy cơ phát hiện quá mức: Một số phần mềm diệt virus có thể tự động xem xét các tệp tin hoặc ứng dụng và cảnh báo người dùng mà không có sự xác nhận chính xác, tạo ra nguy cơ phát hiện quá mức và làm phiền người dùng.

Mặc dù phần mềm diệt virus là một công cụ quan trọng trong việc bảo vệ máy tính, nhưng người dùng cũng cần cân nhắc và tuân thủ các biện pháp cẩn thận để tránh những tác hại tiềm ẩn.[16]

3.2.2 Bức tường lửa cá nhân (Personal Firewall)

` Tường lửa cá nhân (Personal Firewall) không phải một cái gì đó quá xa vời hoặc chỉ dành cho các nhà cung cấp dịch vụ Internet (ISP) mà mỗi máy tính cá nhân cũng cần phải sử dụng tường lửa để bảo vệ trước virus và các phần mềm độc hại. Khi sử dụng tường lửa, các thông tin vào và ra đối với máy tính được kiểm soát một cách vô thức hoặc có chủ ý. Nếu 1 phần mềm độc hại đã được cài vào máy tính có hành động kết nối ra Internet thì tường lửa có thể cảnh báo giúp người sử dụng loại bỏ hoặc vô hiệu hoá chúng. Tường lửa giúp ngăn chặn các kết nối đến không mong muốn để giảm nguy cơ bị kiểm soát máy tính ngoài ý muốn hoặc cài đặt vào các chương trình độc hại hay virus máy tính. Tường lửa được chia thành hai loại chính:

Sử dụng Tường lửa bằng phần cứng: Đối với người sử dụng kết nối Internet thông qua modem hoặc card chuyên dụng, tường lửa phần cứng là một lựa chọn không tồi. Thông thường, chức năng "tường lửa" ở chế độ mặc định của nhà sản xuất được tắt, và người dùng có thể kích hoạt nó bằng cách truy cập vào modem. Tuy tường lửa phần cứng không đảm bảo an toàn tuyệt đối, nhưng chúng thường ngăn chặn kết nối không hợp lệ. Vì vậy, việc sử dụng kết hợp tường lửa phần cứng với tường lửa phần mềm là phổ biến.

Sử dụng Tường lửa bằng phần mềm: Ngay cả hệ điều hành Windows cũng tích hợp sẵn tính năng tường lửa bằng phần mềm. Tuy nhiên, các phần mềm từ các hãng thứ ba thường cung cấp nhiều tính năng hơn và hoạt động hiệu quả hơn so với tường lửa mặc định của Windows. Ví dụ, ZoneAlarm Security Suite của hãng ZoneLab là một bộ công cụ đa nhiệm,

bảo vệ hiệu quả trước virus, phần mềm độc hại, chống spam và cung cấp tính năng tường lửa.[1]

Tường lửa cá nhân (Personal Firewall) mang lại nhiều lợi ích quan trọng trong việc bảo vệ máy tính cá nhân khỏi các mối đe dọa trực tuyến nhưng bên cạnh đó cũng là một vài bất tiện đi song song theo đó. Sau đây là một vài lợi ích và tác hại của tường lửa cá nhân đối với người dùng.

• Lợi ích

Tường lửa cá nhân giúp ngăn chặn các mối đe dọa trực tuyến như virus, một số phần mềm độc hại khác từ việc xâm nhập vào máy tính cá nhân.

Kiểm Soát Kết Nối Mạng: Tường lửa có khả năng kiểm soát và giám sát kết nối mạng đối với máy tính cá nhân. Điều này giúp người dùng theo dõi và quản lý các hoạt động mạng, đồng thời giúp người dùng ngăn chặn kết nối không mong muốn.

Báo cáo và cảnh báo hoạt động đáng ngờ: Tường lửa có thể cung cấp báo cáo và cảnh báo về những hoạt động mạng đáng ngờ hoặc có thể là dấu hiệu của một cuộc tấn công. Điều này giúp người dùng có thể phản ứng kịp thời để bảo vệ hệ thống của mình.

Ngăn chặn kết nối không an toàn: Tường lửa ngăn chặn các kết nối không an toàn và nguy cơ bị tấn công từ các nguồn không đáng tin cậy, giảm khả năng máy tính bị kiểm soát từ xa hoặc bị tấn công mạng.

Bảo vệ dữ liệu cá nhân: Tường lửa cá nhân giữ cho dữ liệu cá nhân của người dùng an toàn bằng cách ngăn chặn truy cập không ổn định từ các nguồn không an toàn.

Kiểm soát quyền truy cập ứng dụng: Tường lửa có khả năng kiểm soát quyền truy cập của các ứng dụng vào mạng, giúp người dùng quản lý chặt chẽ quyền truy cập và tránh các ứng dụng độc hại.

Bảo vệ khỏi các loại tấn công mạng: Tường lửa cá nhân giúp ngăn chặn các loại tấn công mạng như DDoS (Distributed Denial of Service), giữ cho máy tính cá nhân luôn khả dụng và hoạt động bình thường.

Chống Phishing và Spam: Một số tường lửa cá nhân có khả năng phát hiện và ngăn chặn email phishing và spam, giúp bảo vệ người dùng khỏi những mối đe dọa này.[16]

• Tác hại

Cản trở kết nối hợp lệ: Một số tường lửa cá nhân có thể ngăn chặn kết nối hợp lệ, gây khó khăn cho người dùng khi sử dụng các ứng dụng hoặc dịch vụ mạng.

Khả năng báo cáo giả mạo: có thể xảy ra tình trạng tường lửa báo cáo giả mạo, cảnh báo về các hoạt động không đáng ngờ không chính xác, dẫn đến sự nhầm lẫn.

Yêu cầu cấu hình phức tạp: Cấu hình tường lửa có thể là quá trình phức tạp đối với người dùng không có kinh nghiệm, và cài đặt không đúng có thể dẫn đến sự không an toàn.

Tăng chi phí và tài nguyên: Một số tường lửa cá nhân chất lượng cao có thể yêu cầu chi trả một khoản phí, và một số cũng tiêu tốn một lượng tài nguyên hệ thống đáng kể.

Khả năng được vượt qua: Tường lửa cá nhân, mặc dù là một biện pháp an ninh quan trọng, không thể đảm bảo hoàn toàn rằng nó sẽ ngăn chặn mọi mối đe dọa, đặc biệt là trước các kỹ thuật tấn công mới và tiên tiến.

Sự Phức Tạp trong Quản Lý: Việc quản lý và duy trì tường lửa cá nhân đôi khi đòi hỏi kiến thức kỹ thuật cao, đặc biệt là khi cần phải cấu hình các thiết lập chi tiết.

Gây chậm trễ trong kết nối mạng: Các tường lửa có thể gây chậm trễ trong kết nối mạng do quá trình kiểm tra và lọc dữ liệu.

Tuy nhiên, những tác hại trên thường có thể được giảm thiểu thông qua việc chọn lựa và cấu hình đúng loại tường lửa cá nhân, cũng như bằng cách duy trì và cập nhật thường xuyên để đảm bảo tính hiệu quả và an toàn cao nhất.[16]

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

Hệ điều hành Windows, do sự phổ biến của nó, thường xuyên phải đối mặt với các lỗ hổng bảo mật, mở cửa cho khả năng bị tận dụng bởi tin tặc. Các lỗ hổng này có thể là điểm đầu tiên cho việc chiếm quyền điều khiển hoặc triển khai virus và phần mềm độc hại khác. Để đối phó với rủi ro này, việc cập nhật các bản vá lỗi của Windows là quan trọng.

Người sử dụng cần thường xuyên kiểm tra và cập nhật các bản vá bảo mật này thông qua trang web Microsoft Update, bao gồm cả việc nâng cấp tất cả các phần mềm của hãng Microsoft, hoặc thông qua dịch vụ Windows Update dành riêng cho hệ điều hành Windows. Đặt chế độ nâng cấp tự động (Automatic Updates) là một giải pháp tốt nhất để đảm bảo rằng hệ thống của bạn luôn được cập nhật với các bản vá mới nhất.

Tính năng này hỗ trợ các bản Windows mà Microsoft xác nhận là hợp pháp, đồng thời giúp người sử dụng giữ cho hệ điều hành của họ an toàn và bảo mật.[1]

3.2.4 Vận dụng kinh nghiệm sử dụng máy tính

Cho dù sử dụng tất cả các phần mềm và phương thức trên nhưng máy tính vẫn có khả năng bị lây nhiễm virus và các phần mềm độc hại bởi mẫu virus mới chưa được cập nhật kịp thời đối với phần mềm diệt virus. Người sử dụng máy tính cần sử dụng triệt để các chức năng, ứng dụng sẵn có trong hệ điều hành và các kinh nghiệm khác để bảo vệ cho hệ điều hành và dữ liệu của mình[1]. Một số kinh nghiệm tham khảo như sau:

Phát hiện sự hoạt động khác thường của máy tính: Đa phần người sử dụng máy tính không có thói quen cài đặt, gỡ bỏ phần mềm hoặc thường xuyên làm hệ điều hành thay đổi - có nghĩa là 1 sự sử dụng ổn định - sẽ nhận biết được sự thay đổi khác thường của máy tính. Ví dụ đơn giản: Nhận thấy sự hoạt động chậm chạp của máy tính, nhận thấy các kết nối ra ngoài khác thường thông qua tường lửa của hệ điều hành hoặc của hãng thứ ba (thông qua các thông báo hỏi sự cho phép truy cập ra ngoài hoặc sự hoạt động khác của tường lửa). Mọi sự hoạt động khác thường này nếu không phải do phần cứng gây ra thì cần nghi ngờ sự xuất hiện của virus. Ngay khi có nghi ngờ, cần kiểm tra bằng cách cập nhật dữ liệu mới nhất cho phần mềm diệt virus hoặc thử sử dụng 1 phần mềm diệt virus khác để quét toàn hệ thống.[16]

Kiểm soát các ứng dụng đang hoạt động: Kiểm soát sự hoạt động của các phần mềm trong hệ thống thông qua Task Manager hoặc các phần mềm của hãng thứ ba (chẳng hạn: ProcessViewer) để biết 1 phiên làm việc bình thường hệ thống thường nạp các ứng dụng nào, chúng chiếm lượng bộ nhớ bao nhiêu, chiếm CPU bao nhiêu, tên file hoạt động là gì... ngay khi có điều bất thường của hệ thống (dù chưa có biểu hiện của sự nhiễm virus) cũng có thể có sự nghi ngờ và có hành động phòng ngừa hợp lý. Tuy nhiên cách này đòi hỏi 1 sự am hiểu nhất định của người sử dụng.[1]

Loại bỏ một số tính năng tự động của hệ điều hành có thể tạo điều kiện cho sự lây nhiễm virus: Theo mặc định Windows thường cho phép các tính năng tự chạy (autorun) giúp người sử dụng thuận tiện cho việc tự động cài đặt phần mềm khi đưa đĩa CD hoặc đĩa USB vào hệ thống. Chính các tính năng này được một số loại virus lợi dụng để lây nhiễm ngay khi vừa cắm ổ USB hoặc đưa đĩa CD phần mềm vào hệ thống (một vài loại virus lan truyền rất nhanh trong thời gian gần đây thông qua các ổ USB bằng cách tạo các file autorun.inf trên ổ USB để tự chạy các virus ngay khi cắm ổ USB vào máy

tính). Cần loại bỏ tính năng này bằng các phần mềm của hãng thứ ba như TWEAKUI hoặc sửa đổi trong Registry.

Quét virus trực tuyến: Sử dụng các trang web cho phép phát hiện virus trực tuyến.[1]

3.3 Bảo vệ dữ liệu máy tính

Nếu như không chắc chắn 100% rằng có thể không bị lây nhiễm virus máy tính và các phần mềm hiểm độc khác thì bạn nên tự bảo vệ sự toàn vẹn của dữ liệu của mình trước khi dữ liệu bị hư hỏng do virus (hoặc ngay cả các nguy cơ tiềm tàng khác như sự hư hỏng của các thiết bị lưu trữ dữ liệu của máy tính). Dưới đây là một số cách bảo vệ dữ liệu máy tính:

3.3.1 Bảo vệ dữ liệu hệ thống

Mã hóa dữ liệu của người dùng: Mã hóa dữ liệu là rất quan trọng, đặc biệt nếu bạn lưu trữ thông tin có độ nhạy cảm cao trên thiết bị của mình. Trong trường hợp bạn bị mất thiết bị và thông tin rơi vào tay kẻ xấu, dữ liệu của bạn sẽ được an toàn. Bạn có thể sử dụng phần mềm BitLocker để mã hóa dữ liệu của mình. Để truy cập vào BitLocker, hãy truy cập vào Control Panel (Bảng điều khiển) → System and Security (Hệ thống và bảo mật) → BitLocker Drive Encryption (Mã hóa ổ đĩa BitLocker) và bật BitLocker bằng cách nhấp vào Enable BitLocker (Kích hoạt BitLocker).

Chỉ tải xuống và cài đặt các ứng dụng đã được xác minh: Tránh tải xuống và cài đặt ứng dụng từ các nguồn chưa được xác minh. Hãy chắc chắn tải xuống ứng dụng từ các trang web chính thức và được xác minh. Trong trường hợp của Windows 10, cửa hàng ứng dụng được Microsoft xác minh và đảm bảo rằng các ứng dụng không chứa mã độc. Windows 10 có một tính năng ngăn người dùng cài đặt ứng dụng từ bất kỳ nguồn chưa được xác minh nào ngoại trừ Microsoft Store. Tính năng này đảm bảo rằng không có chương

trình độc hại nào có thể được tự động tải xuống và nhúng vào máy tính của bạn mà không có sự đồng ý của bạn. Một cách khác để bảo vệ dữ liệu của bạn khỏi tin tặc trong Windows 10 là sử dụng tài khoản người dùng tiêu chuẩn thay vì tài khoản quản trị viên. Điều này cũng ngăn chặn mã độc cố gắng truy cập bằng cách lợi dụng trạng thái của tài khoản quản trị viên. Từ đó, chúng tạo ra một tài khoản quản trị viên mới, sau đó từ tài khoản mới này sẽ thay đổi tài khoản ban đầu thành tài khoản tiêu chuẩn.[15]

Tắt theo dõi quảng cáo: Tin tặc có thể theo dõi các xu hướng trực tuyến của bạn trong khi duyệt Internet. Người bán sử dụng điều này để tạo hồ sơ người dùng của bạn dựa trên lịch sử duyệt web của bạn. Họ sử dụng nó để gửi cho các công ty quảng cáo dựa trên thông tin thu thập được. Vì vậy, để đảm bảo an toàn bạn có thể tắt nó bằng cách vào Settings (Cài đặt) →Privacy settings (Cài đặt bảo mật) → tùy chọn General → disable all.[14]

3.3.2 Bảo vệ dữ liệu đầu ra

Đăng xuất tài khoản sau khi kết thúc hoạt động: Một trong những cách đơn giản nhất để bảo mật dữ liệu máy tính là đăng xuất mọi tài khoản sau khi kết thúc hoạt động, đặc biệt là khi sử dụng máy tính công cộng. Hành động này không chỉ đơn thuần là việc đăng xuất khỏi hệ thống, mà còn là việc xác nhận sự tỉnh táo và quan tâm đối với khía cạnh bảo mật thông tin cá nhân của bạn. Duy trì kết nối không cần thiết có thể đặt bạn vào mối nguy hiểm, khi thông tin của bạn có thể bị khai thác bởi những tội phạm công nghệ thông qua những lỗ hổng về an ninh mạng. Trái với việc thường xuyên tiến hành đăng xuất sau khi sử dụng dịch vụ, việc giữ kết nối liên tục có thể tạo điều kiện thuận lợi cho việc truy cập trái phép vào tài khoản của bạn, khi các kẻ xâm nhập có thể tận dụng sự bất cẩn để truy xuất thông tin nhạy cảm.

Tuyệt đối không click vào các link lạ: Sử dụng mạng xã hội thường xuyên sẽ khó có thể tránh khỏi tình huống nhận được những đường link lạ và

yêu cầu nhấn vào đường link. Việc không may truy cập vào những liên kết không rõ nguồn gốc này có thể tạo cơ hội cho những kẻ xấu để lấy cắp thông tin quý báu của bạn. Mặc dù đây là một chiêu trò lừa đảo khá cũ nhưng vẫn có rất nhiều người dùng bị mắc phải. Để đảm bảo tính an toàn trước khi bạn mở một liên kết nào đó, có thể thực hiện kiểm tra tên miền trước đó bằng công cụ tìm kiếm của Google. Nhờ vào điều này, bạn có thể biết được mức độ uy tín và đáng tin cậy của liên kết mà bạn định truy cập.

Xóa Browser History và Cookies thường xuyên: Khi bạn tham gia mạng xã hội, thực hiện thanh toán trực tuyến, thậm chí tìm kiếm các bộ phim trên web, nó cũng sẽ để lại một chút thông tin liên quan đến cá nhân bạn. Những nội dung này chứa đựng những liên kết đã truy cập, thông tin đăng nhập đã được ghi nhớ trên ứng dụng trình duyệt.Nếu bạn là một người có kiến thức về lĩnh vực máy tính, công nghệ thì bạn sẽ dễ dàng việc xóa bỏ Browser history và cookies thường xuyên để tránh bị theo dõi hoạt động thường ngày của bạn.[16]

3.4 Gợi ý một số phần mềm duyệt Virus

• McAfee AntiVirus Plus

Đứng đầu trong top các phần mềm chặn virus trên web phải kể đến McAfee AntiVirus Plus. Là một trong những phần mềm sánh ngang với các "ông lớn diệt virus" trong ngành như Kaspersky, Norton,… về chất lượng. McAfee có ưu điểm: Chặn hầu hết các cuộc tấn công zero-day và các mã độc phổ biến; Tối ưu hóa hiệu suất và trình quản lý mật khẩu cá nhân; Có khả năng tương thích đa thiết bị,….

Hình 3.4.1 McAfee AntiVirus Plus [17]

• Sophos Home Premium

Sophos Home Premium sử dụng công nghệ Deep Learning để phát hiện các mối đe dọa từ các mã độc trước khi chúng kịp tấn công hệ thống máy tính của bạn. Sophos Home Premium có trình quét và dọn dẹp virus mạnh mẽ, giúp xóa bỏ mọi dấu vết của phần mềm độc hại chạy ngầm một cách triệt để nhất.

Hình 3.4.1 Sophos Home Premium [18]

• Avast Free Antivirus

Là bản miễn phí nhưng người dùng phải tiến hành đăng ký để nhận mã bản quyền sử dụng một năm (trước khi thời hạn dùng thử 30 ngày kết thúc). Avast có giao diện đẹp mắt với tính năng chống lại phần mềm gây

hại, phòng tránh lây nhiễm qua e-mail, chat, ngăn chặn tấn công từ các website chứa mã độc…

Hình 3.4.3 Avast Free Antivirus [19]

TÓM TẮT CHƯƠNG 3

Chương này sẽ bắt đầu bằng việc phân tích các biểu hiện của máy tính bị nhiễm virus máy tính. Qua đó, phát hiện ra dấu hiệu đặc thù khi máy tính nhiễm virus, từ các hiện tượng hiển nhiên đến những biểu hiện nhỏ và các đuôi tệp có khả năng bị nhiễm virus. Bằng cách này, người đọc có được cái nhìn tổng quan về cách nhận diện sự nhiễm virus và hậu quả của nó đối với hệ thống máy tính. Tiếp theo, chương chuyển qua các biện pháp phòng chống virus máy tính. Một số biện pháp bảo vệ được đề cập bao gồm sử dụng phần mềm diệt virus, thiết lập bức tường lửa cá nhân, cập nhật và sửa chữa lỗi hệ điều hành, cũng như việc áp dụng kinh nghiệm sử dụng máy tính. Các giải pháp này đều nhằm mục đích ngăn chặn sự lây lan của virus và bảo vệ hệ thống khỏi những tổn thất không mong muốn. Cuối cùng, chương đưa ra một số gợi ý về các phần mềm diệt virus hiệu quả, giúp người lựa chọn công cụ phù hợp để bảo vệ máy tính của họ và cung cấp một hệ thống toàn diện về cách phát hiện, ngăn chặn và giải quyết vấn đề virus máy tính.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

• KẾT LUẬN

Trong giai đoạn hiện nay, virus máy tính đã trở thành một trong những thách thức đáng kể đối với an toàn và bảo mật thông tin. Sự tiện lợi và kết nối liên mạng của máy tính mang lại nhiều cơ hội cho sự phát triển của virus, đặt ra những rủi ro nghiêm trọng cho cả người sử dụng cá nhân và tổ chức. Để đối mặt với mối đe dọa này, việc thực hiện các biện pháp phòng chống là không thể phủ nhận. Sự chú ý và nhận thức về những chiến lược bảo mật là yếu tố then chốt. Sử dụng phần mềm diệt virus mạnh mẽ và duy trì các hệ thống an ninh mạng là quan trọng để ngăn chặn sự lây lan của virus và malware.

Hơn nữa, việc hướng dẫn người sử dụng về nguy cơ bảo mật và cách nhận diện các mối đe dọa cũng đóng vai trò quan trọng. Sự cảnh báo và kiến thức vững về an toàn thông tin sẽ giúp tạo nên một môi trường trực tuyến an toàn hơn. Tuy nhiên, cần lưu ý rằng bảo mật là một quá trình không ngừng, và những biện pháp cần phải được cập nhật và cải tiến theo thời gian để đối phó với những thách thức mới.

Chính vì thế bài tiểu luận này đóng góp một phần quan trọng trong việc tìm hiểu về kiến thức liên quan đến Virus máy tính, trong đó bao gồm việc tìm hiểu về cách hoạt động cũng như sự nguy hại và biện pháp trong việc phòng chống các thiết bị khỏi sự xâm lược của Virus máy tính.

• HẠN CHẾ

Đề tài ***"Virsu máy tính hiện nay và biện pháp phòng chống"*** là một chủ đề khá rộng, với thời gian thực hiện đề tài tương đối hạn chế nên sẽ không thể tránh được những thiếu sót nhất định. Một số khía cạnh của đề tài có thể chưa được xem xét sâu rộng đủ, và dữ liệu có thể chưa đầy đủ. Tuy nhiên, tiểu luận này đã cố gắng trình bày một cái nhìn tổng quan về Virus và

một số biện pháp để phòng chống. Nó có thể sẽ giúp mở ra cơ hội để tìm hiểu sâu hơn và nghiên cứu các khía cạnh cụ thể hơn về các Virus khác.

• HƯỚNG PHÁT TRIỂN

Đối mặt với sự tiến triển không ngừng của công nghệ và sự nguy hiểm ngày càng tăng của virus máy tính, biện pháp phòng chống và bảo mật thông tin đang trở thành một lĩnh vực đầy thách thức và đòi hỏi sự đổi mới liên tục. Trong tương lai, các biện pháp sau có thể được cải tiến và mở rộng để bảo vệ mạng lưới và dữ liệu người dùng chẳng hạn như trí tuệ nhân tạo, Blockchain, bảo mật vân tay, nhận diện khuôn mặt,.. hoặc sẽ có thêm nhiều phần mềm mới gần gũi với người dùng hơn trong tương lai. Nếu có cơ hội, em cũng rất muốn được tìm hiểu chuyên sâu thêm trong các vấn đề ấy.

TÀI LIỆU THAM KHẢO

[1] Wikipedia Virus máy tính

[2] John Aycock, *Computer Virus and Malware* Springer; 2006th edition (July 20, 2006)

[3] Haris A.Khan, Ali Syed, Azeem Mohammad, Maika N. Halgamuge *Computer Virus and Protection Methods Using Lab Analysis*.

[4] Imran KhanAn introduction to computer viruses: *Problems and solutions*.

[5] Anand Mylavarapu, Anil Chukkapalli, *Source code analysis and performance*, Computer Science Department, St. Cloud State University.

[6] Wanderlustsaxshy Learn geeksf for geeksf *What is Browser Hijacking Software ?*

[7] Cynthia Wong, Stan Bielski, Jonathan M. McCune, Chenxi Wang, *A Study of Mass-mailing Worms*, Carnegie Mellon University.

[8] David Harley, Robert Slade, Urs Gattiker (2001), *Viruses Revealed*, McGraw Hill.

[9] P. Szor, *"The art of computer virus research and defense"*, Pearson Education, 2005.

[10] F. Cohen, *"Computer viruses: theory and experiments"*, Computers & security, vol. 6, no. 1, pp. 22-35. 1987.

[11] Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard Malware Analyst's Cookbook and DVD: *Tools and Techniques for Fighting Malicious* Codepublished on September 20, 2010.

[12] Kevin Mitnick and William L. Simon Ghost in the Wires: My Adventures as the World's Most Wanted Hacker publishesd August 15, 2011.

[13] *Reza Azarmsa Computer Viruses and Safe Educational Practices* Vol. 31, No. 11 (November 1991).

[14] P. Szor, *"The art of computer virus research and defense"*, Pearson Education, 2005

[15] N. Nissim, R. Moskovitch, L. Rokach and Y. Elovici, "*Detecting unknown computer worm activity via support vector machines and active learning"*, Pattern Analysis and Applications, vol 15, no. 4, pp. 459-475, 20

[16] Alexander N. Stadnik, Kirill S. Skryl, Ivan I. Korovin, Alexey V. *Astrakhov Exploration of the use of temporary computer system* resources by anti-virus tools

[17] Wikipedia McAfee AntiVirus Plus

[18] Wikipedia Sophos

[19] Wikipedia Avast Antivirrus