ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC SÀI GÒN

TRẦN BÙI TY TY

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

TIỂU LUẬN
NGÀNH:CÔNG NGHỆ THÔNG TIN

Thành phố Hồ Chí Minh, năm 2023

ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC SÀI GÒN

TRẦN BÙI TY TY

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

ĐỀ CƯƠNG TỂU LUẬN HỆ ĐIỀU HÀNH
NGÀNH:CÔNG NGHỆ THÔNG TIN

Người hướng dẫn khoa học:

TS. PHAN TẤN QUỐC

Thành phố Hồ Chí Minh, năm 2023

LỜI CAM ĐOAN

Tôi tên là Trần Bùi Ty Ty, cam đoan rằng:

- Những kết quả nghiên cứu được trình bày trong tiểu luận là công trình của riêng tôi dưới sự hướng dẫn của TS.Phan Tấn Quốc

- Những kết quả nghiên cứu của các tác giả khác và các số liệu được sử dụng trong tiểu luận đều có trích dẫn đầy đủ, chính xác và trung thực.

- Những kết quả nghiên cứu chung (tác giả có tham gia) được trình bày trong tiểu luận đều có sự đồng ý của các đồng tác giả.

- Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung bài tiểu luận của mình.

LỜI CÁM ƠN

Chúng tôi xin bày tỏ lòng biết ơn đến các thầy cô giáo trong khoa Công nghệ thông tin - Trường Đại học Sài Gòn, những người đã truyền đạt kiến thức chuyên môn và phương pháp làm việc khoa học \. Cũng như lời cảm ơn đến các nhà nghiên cứu, chuyên gia trong bảo mật mạng đã cung cấp thông tin cần thiết, chia sẻ kiến thức về Virus cũng như các phương pháp để khắc phục, để chúng tôi có thể tham khảo và phát triển, hoành thành bài tiểu luận này.

Tiểu luận này đã giúp chúng tôi nắm bắt được sự nguy hại của Virus máy tính, đồng thời biết được các phương pháp để phòng chống cũng như khắc phục hậu quả do Virus gây ra. Chúng tôi hy vọng thông qua bài tiểu luận này, chúng tôi đã đóng góp một phần nhỏ trong việc nâng cao nhân thức của mọi người về vấn đề này và có thể phòng chống Virus một cách hiệu quả hơn.

MỤC LỤC

MỞ ĐẦU

1 Lý do chọn đề tài

-Sự phát triển nhanh chóng của khoa học 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.Các virus máy tính hiện nay không chỉ đơn giản là các chương trình có hại, mà chúng đã tiến hóa và trở nên nguy hiểm hơn. 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. Với tình hình này, việc hiểu rõ về các virus máy tính và biểu hiện khi máy tính bị nhiễm virus trở nên cực kỳ quan trọng.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.

2. Lịch sử nghiên cứu vấn đề

3. Mục đích nghiên cứu

Chúng tôi sẽ tập trung nghiên cứu và chia làm 4 mục tiêu chính

- Phân tích, nghiên cứu sâu về các loại Virus đang hoành hành hiện nay: Tiểu luận này sẽ phân tích sâu về các loại Virus phổ biến nhất hiện nay và những trở ngại mà người dùng gặp phải khi máy tính bị nhiễm Virus. Chúng tôi sẽ tập trung nghiên cứu về nguyên nhân và quá trình xuất hiện của các loại Virus này

- Nghiên cứu các hình thức lây lan và phát triển của các Virus: Ở phần này chúng tôi sẽ nghiên cứu về các phương tiện mà virus lây lan qua các thiết bị máy tính của người dùng, các phần mềm, tập tin mà Virus dễ dàng xâm chiếm và hoành hành. Đồng thời nghiên cứu quá trình phát triển và những biến thể của các Virus máy tính

- Tìm hiểu các biểu hiện và phương pháp phòng chống Virus: Chúng tôi sẽ trình bày một số đặc điểm đặc trưng của một máy tính khi bị nhiễm Virus để phòng chống. Bên cạnh đó tiểu luận này sẽ giới thiệu một số biện pháp phòng chống Virus trực tiếp trên máy chủ, máy tính cá nhân, cùng với một số phần mềm giúp truy xuất và tiêu diệt Virus

- Tầm quan trọng của vấn đề: Cuối cùng chúng tôi sẽ nhấn mạnh một số tầm quan trọng của việc hiểu biết về các loại Virus cũng như biện pháp phòng chống đề phòng các rủi ro không đáng có.

4. Đối tượng nghiên cứu và phạm vi nghiên cứu

3.1 Đối tượng nghiên cứu

- Người dùng máy tính cá nhân: chúng tôi tập trung vào tất cả các đối tượng người dùng máy tính các nhân, bất kể trình độ kỹ thuật của họ, để giúp họ hiểu hơn về các nguy cơ từ Virus máy tính và cách bảo vệ mình

- Doanh nghiệp và tổ chức: Các doanh nghiệp và tổ chức cũng là đối tượng nghiên cứu quan trọng, vì họ phải đối mặt với các mối đe dọa từ virus máy tính và có nhu cầu bảo vệ dữ liệu quan trọng của họ.

3.2 Phạm vi nghiên cứu

- Các loại virus đang hoành hành: Tiểu luận này sẽ tập trung chủ yếu vào một số Virus phổ biến hiện nay và các mối đe dọa trực tuyến khác.

- Biện pháp, các phần mềm diệt Virus: Chúng tôi sẽ xem xét và đưa ra một vài biện pháp, phần mềm hỗ trợ phù hợp cho từng đối tượng nhằm mục đích ngăn chặn và loại bỏ các Virus máy tính

5. Phương pháp nghiên cứu

4.1 Mục tiêu nghiên cứu

- Điều tra tình hình hiện tại của các loại virus máy tính phổ biến trong giai đoạn hiện nay và nắm bắt các đặc điểm quan trọng của chúng.Điều này bao gồm việc xác định các loại virus máy tính được phát hiện gần đây, tần suất xuất hiện, và cách chúng hoạt động.

- Xác định các biện pháp phòng chống hiện tại và các chiến lược bảo mật mạng được sử dụng để đối phó với các loại virus máy tính này. Chúng tôi

đã tập trung vào việc tìm hiểu về các biện pháp và chiến lược hiện tại để ngăn chặn và xử lý các cuộc tấn công từ virus máy tính.

- Đề xuất các biện pháp phòng chống và cải tiến để tăng cường bảo mật mạng trong bối cảnh của các mối đe dọa mới. Chúng tôi đã nghiên cứu và đề xuất các biện pháp bảo mật mới dựa trên những hiểu biết và phân tích của chúng tôi.

4.2 Phương pháp thu thập dữ liệu

- Thu thập thông tin từ các nguồn tài liệu như sách, bài viết khoa học, báo cáo từ các tổ chức an ninh mạng, và trang web chính thống về bảo mật mạng. Chúng tôi đã tìm hiểu thông tin từ các nguồn chính thống để xây dựng cơ sở kiến thức về các loại virus máy tính và biện pháp phòng chống.
- Tìm hiểu về các tài liệu đã xuất bản và nhận diện các xu hướng và dữ liệu thống kê quan trọng về các loại Virus máy tính và biện pháp phòng chống. Chúng tôi đã đánh giá và phân tích dữ liệu thống kê để xác định xu hướng và mức độ nguy hiểm của các loại virus máy tính.

4.3 Phương pháp phân tích dữ liệu

- Sử dụng phân tích nội dung để phân tích các tài liệu thu thập từ các nguồn tài liệu chính thống.
- Áp dụng phân tích thống kê để xác định xu hướng, biến đổi, và sự phân bố của các loại virus máy tính và biện pháp phòng chống.
- Tổng hợp các thông tin tìm được từ các nguồn tài liệu kết hợp với thông tin thực tế hiện nay mà phân tích đưa ra biện pháp thích hợp nhất.

4.4 Độ tin cậy và độ hợp lý

- Để đảm bảo tính đáng tin cậy của nghiên cứu, chúng tôi đã thực hiện kiểm tra lại dữ liệu và thông tin từ nhiều nguồn khác nhau để đảm bảo tính chính xác và độ tin cậy của dữ liệu.

- Các biện pháp đảm bảo độ hợp lý bao gồm việc sử dụng phương pháp nghiên cứu được công nhận và kiểm tra kỹ thuật của cuộc khảo sát để đảm bảo tính đáng tin cậy của kết quả.

4.5 Phương pháp tham khảo

- Danh sách các nguồn tham khảo bao gồm tài liệu từ các nguồn tài liệu như sách, bài viết khoa học, báo cáo từ tổ chức an ninh mạng, và trang web chính thống về bảo mật mạng

6. Cấu trúc của tiểu luận

-Ngoài phần mở đầu, kết luận, danh mục tài liệu tham khảo và phụ lục, tiểu luận gồm có 3 chương:

Chương 1: Chúng tôi sẽ trình bày về khái niệm của Virus máy tính, đồng thời mô tả một số tính chất 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.

- 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. 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..

• **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
```

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 (Visual Basic for Applications)[3] 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.

- 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.

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.

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 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.

- 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.

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.

1.2.3 - **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.

1.2.4 Virus Macro

- Trong thuật ngữ máy tính , vi-rút macro là vi-rút 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 . Nhiềuchương trình chống vi-rút có thể phát hiện vi-rút macro; tuy nhiên, hành vi của virus macro vẫn có thể khó phát hiện.

- **Cách thức hoạt động của Virus Macro:**

• Khi một tệp chứa vi-rút 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, vi-rút 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.

1.2.5 Virus đa phần (Multipartite Virus)

- Một vi-rút 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.

1.2.6 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.

- **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).

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

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.

- 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.

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.

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.

- 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.

- 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 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

- 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.

• **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.

2.3. Tác động của Virus đến đời sống, thiết bị

- 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 sông:

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.

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.