BÀN VỀ MỘT SỐ LOẠI VIRUS TIN HỌC HIỆN NAY.

NGÔ ANH VŨ

Hiện nay, hiện tượng lan tràn " Virus " tin học đang làm cho không ít người lo ngại. Việc không lường trước những hậu quả do nó mang lại đã làm hạn chế việc trao đổi các phần mềm ứng dụng.

Bài viết này chỉ nhằm đưa ra một số nhận định về virus có tại thành phố Hồ Chí Minh .

1. Phân loại virus .

Căn cứ vào cách lây lan của virus trên máy, ta có thể chia làm 2 loại sau :

a. B-virus :

Là loại virus chỉ lây lan thông qua Boot sector. Thật vậy khi khởi động, máy tiến hành đọc thử 1 sector vào trong vùng nhớ, đó là Boot sector. Việc đọc vào một Boot sector đã bị nhiễm sẽ dẫn đến sự chi phối của virus ngay từ khi khởi động máy .

Đặc trưng của loại virus này có thể kể ra là Stoned virus với câu thông báo " Your PC is now stoned ", hay loại (C) Brain từng gây khó chịu một thời đã được cải tiến tới version 9.2 .

b. F-virus :

Là loại virus lây lan thông qua các chức năng của DOS khi thực hiện một File thi hành được (Executable). Việc thi hành 1 file đã bị nhiễm sẽ dẫn đến sự lây lan sang một file khác hoặc sẽ tạo ra một mầm bệnh trong vùng nhớ mà bất kỳ một file nào khác khi thi hành sẽ bị lây lan .

Nếu đối với B-virus, việc lây tiến hành trên Boot sector,thì F-virus lại lây bằng cách "gắn" đuôi từng file .

Điển hình cho loại virus này là virus " cổ xưa " 1701, 534 (Tên được đặt theo kích thước chương trình của virus đó) và "hiện đại" như Eddie (còn được gọi là Dark Avenger) v.v..

Việc phân chia loại virus này chỉ mang tính chất tương đối vì hiện nay đã xuất hiện loại F-virus có khả năng lây trên Boot sector (được gọi dưới tên Fixed disk virus), và trong tương lai sẽ có một chuyên gia nào đó tìm ra một cách lây lan đặc sắc hơn.

2. Các đặc trưng của virus .

a. Tính phá hoại

Đây là đặc tính nổi bật nhất vì virus ra đời không ngoài mục đích phá hoại.Sự xuất hiện một loại virus mới thường mang lại mối lo ngại cho nhiều người nhất là khi tính phá hoại của chúng chưa được khảo sát cặn kẽ .

Đối tượng của sự phá hoại thường nhằm vào các thiết bị ngoại vi như màn hình, đĩa từ (đĩa mềm,đĩa cứng).Sự phá hoại đôi khi chỉ đơn giản bằng cách tăng kích thước file, đổi lại ngày tháng năm của file cho đến việc gây "mưa" trên màn hình, đổi tên đĩa v.v..

Càng ngày tính phá hoại càng phong phú và gia tăng đáng sợ. Mặt khác, sự sao chép các virus vì một lý do nào đó gặp lỗi (lỗi trong việc ghi ra đĩa hay do cố tình " cải biên " lại) sẽ gây ra một tác hại không lường trước được và làm khó khăn cho việc phòng chống .

b / Tính lây lan .

Như đã nêu trên, việc lây lan tiến hành qua 2 ngõ :Boot sector và File. Để bảo đảm sự tồn tại và phát triển của mình bất kỳ virus nào cũng đòi hỏi phải có được tính chất này. Việc lây lan giữa file này sang file khác hay giữa đĩa này sang đĩa khác đôi khi làm khó chịu hay âu lo cho người sử dụng, và hơn nữa còn gây khó khăn cho việc chữa trị.

Đối với loại B-virus việc lây qua Boot sector tương đối khó khăn vì lẽ kích thước 1 sector không phải là lý tưởng cho một virus có "tầm cỡ ". Chính vì vậy, việc thiết kế 1 virus gọn nhẹ, hữu hiệu gặp nhiều khó khăn. Điển hình cho loại này là virus Marijuana (còn được gọi dưới tên Stoned virus). Với kích thước nhỏ bé nằm gọn trong Boot sector, virus lây được đĩa cứng lẫn mềm, nổi tiếng với câu thông báo " Your PC is now stoned ! "

Để giải quyết khó khăn nói trên, một hướng mới đã phát sinh : Tạo ra virus có 2 phần : Đầu virus và thân virus . Đầu virus nằm gọn trong Boot sector có nhiệm vụ hết sức đơn giản là tải phần thân virus vào và sau đó trao quyền điều khiển.Điển hình cho cách thức này là Virus Brain.

Đối với F-virus, việc lây lan tương đối dễ dàng vì " gắn " phần thân virus vào sau file không phải là việc làm khó k . Ưu điểm của loại virus này là dễ lây lan xa hơn loại B-virus c việc copy lẫn nhau giữa những phần mềm thông dụng hay những trò chơi đã bị nhiễm virus.

Việc lây lan trong F-virus có thể tiến hành bằng 2 cách :

- Khi 1 file đã bị nhiễm được thi hành, nó tìm ngay các file khác trong cùng một thư mục và tiến hành "gắn đuôi " .Tuy nhiên hình thức này không được ưa chuộng lắm vì thời gian gắn đuôi sẽ bị kéo dài nếu có nhiều file thi hành được trong thư mục.Mặt khác, khi chấm dứt việc thi hành file này cũng chấm dứt nguy cơ lây lan cho file khác. Điển hình cho cách thức này là virus 534.

- Khi 1 file đã bị nhiễm được thi hành, nó tiến hành "dọn " một chỗ trong vùng nhớ và đặt vào đó 1 bản sao của mình.Việc thi hành những chương trình tiếp theo đều bị lây lan .Sự lây lan không chỉ xảy ra trong một thư mục xác định mà mọi file đều có nguy cơ bị lây như nhau. Điển hình cho F-virus kiểu này là virus 1701,Eddie v.v..

c:/ Tính duy nhất .

Chẳng rõ xuất phát từ một sai lầm hay từ một biểu hiện của tính khoa học mà hầu hết virus đều có tính chất này : không quá 1 virus cùng loại trên 1 file hay đĩa (xin hiểu nếu chỉ xét file / đĩa chỉ bị nhiễm 1 loại virus). Tính duy nhất này được virus kiểm tra mỗi khi nắm quyền chi phối trên máy.

Việc kiểm tra này hoặc chỉ đơn giản bằng việc kiểm tra một giá trị khóa nào đó (như Brainy9.0 kiểm tra giá trị W[4]=1234h ,Stoned virus với giá trị 2 byte đầu tiên) hay phức tạp hơn bằng cách so sánh toàn bộ thân virus với " đối tượng " có nghi ngờ (như virus Eddie) và nếu có sự sai khác sẽ dẫn đến việc lây lan lập tức .

Tuy nhiên hiện nay với sự quan tâm ngày càng rộng rãi của giới tin học thành phố, việc cải biên lại các virus này đã tạo ra những virus "cải tiến"không đếm xỉa gì đến việc kiểm tra và do đó sự lây lan còn khủng khiếp hơn (chúng tôi đã thấy một bản virus cải biên của Brain 9.2 dưới tên gọi Fixed Virus và một bản virus cải biên của 1701 đã thay phần kiểm tra bằng các lệnh NOP)

Ngoài các đặc tính nói bật trên,ta còn có thể nêu lên một số đặc tính khác, đôi khi chỉ xuất hiện trên một vài loại virus nhưng vẫn mang tính đặc trưng .Đó là :

d/ . Tính bảo mật .

Việc bảo mật chỉ xuất hiện ở các loại virus " xưa " kiểu 1701 .Mục đích của công tác bảo mật nhằm gây khó khăn cho việc chữa trị và đọc chương trình virus .Tuy nhiên việc bảo mật xét ra không cần thiết vì để đọc được một chương trình virus dưới dạng mã máy không phải là một chuyện dễ dàng, và nếu là một chuyên gia thì vấn đề mã hóa cũng không phải là vấn đề phức tạp .Do đó những virus về sau đã "quên" mất đặc tính này .Tuy vậy, gần đây với version mới của Brain (v9.2),dù phần bảo virus không mã hóa nhưng nó đã tránh sự khoa trương của những version trước và cố tình gây khó khăn cho người nhận diện bằng cách chỉ điền chương trình của mình vào những nơi cần thiết và thực chất phần chương trình này chỉ có 200h - 133h = 67h bytes.

e/. Tính sống còn

Là đặc tính tương đối nhỏ, tuy nhiên vẫn đảm bảo cho virus một "sức mạnh " để hồi sinh nếu bị một chương trình nào đấy vô tình hay cố ý làm mất tác dụng của nó. Hiện nay, chỉ có virus Eddie là có đặc tính này.

f/. Tính kế thừa.

Mỗi loại virus ra đời càng muộn càng tiếp thu những cái hay của virus trước đó và cố gắng khắc phục nhược điểm đã bị phát hiện ngăn ngừa. Việc kế thừa có thể xảy ra trong cùng một virus (Brain v9.0 1986 , Brain v9.2 1988) hay giữa các virus khác nhau.

Tiêu biểu cho đặc tính này là các version của virus Brain. Với loại v9.0 ra đời năm 1986, Brain chỉ lây lan giữa các đĩa mềm 360 kb , việc phá hoại chỉ là đổi tên đĩa thành (c) Brain,việc kiểm tra là w[4]=1234h. Khi đã có vacine chống Brain hữu hiệu thì một version mới đã ra đời. Với việc kiểm tra w[3eh]=1234h nó đã vô hiệu hoá mọi loại vacine trị v 9.0 , đó là Brain 9.2 năm 1988. Ngoài tác dụng tương tự trên đĩa mềm nó còn bổ sung bằng việc cho phép lây lan trên đĩa cứng và phá hoại mọi file. Vì lý do này, sự lây lan còn dữ dội hơn.

3/. Phòng chống virus :

Việc phòng chống có thể cũng được chia làm 2 loại :

a/. Chống ngay từ đầu :

Máy sau khi khởi động sẽ thi hành một phần mềm cho phép ngăn chặn mọi file/đĩa đã bị nhiễm virus bằng cách không thực hiện file này và đưa ra câu thông báo.

Điển hình cho loại này hiện nay là phần mềm SCANRES : cho phép phát hiện đến 41 loại virus khác nhau (tuy nhiên vẫn không phát hiện được Brain 9.2) hay Turbo Anti - Virus version 1.0 ....

Việc phòng chống này dù bề ngoài có vẻ chủ động nhưng thực chất vẫn là thụ động vì chỉ có thể chống được những virus đã biết. Khi danh sách virus ngày càng dài ra, các phần mềm Anti Virus lại có những version mới bổ sung. Dù vậy việc triển khai các vacine này thường là chậm trễ khi virus đã lây lan khắp nơi.

b/. Trị file/đĩa bị nhiễm

Cũng như loại trên, thuốc đặc trị vẫn xuất hiện sau khi virus đã có mặt khắp mọi nơi và mức độ "chống chéo" của các loại virus lên nhau càng làm rắc rối cho việc phòng chống.

Cũng vì hai loại chống trả thụ động như trên, việc chống lây lan hữu hiệu nhất hiện nay vẫn là " co cụm " lại bằng cách trao đổi nội bộ chứ không trao đổi phần mềm giữa các trung tâm tin học với nhau.

Tuy vậy , biện pháp này vẫn chưa phải hữu hiệu nhất, cần phải nêu ra ở đây một số yêu cầu tối thiểu mà mỗi phòng máy cần có :

- Luôn khởi động máy bằng đĩa cứng (nếu có thể), hay bằng đĩa boot chuẩn của phòng máy có gắn nhãn chống ghi.
- Không sử dụng bất kỳ một phần mềm mới nào, nhất là trò chơi, nếu không biết rõ xuất xứ; kiểm tra các phần mềm này bằng các vacine đã có.
- Tạo bản sao cho bất kỳ file nào nếu cần lưu trữ.
- Tiến hành kiểm tra và diệt virus bằng các vacine hiện có theo định kỳ.
- Nếu có điều gì bất thường phải ngưng máy và báo ngay cho người có trách nhiệm

Các yêu cầu này phải được thực hiện một cách nghiêm túc khi vào phòng máy.

Tóm lại, mục đích của bài này chỉ nhằm nêu sơ lược một ít đặc trưng của tình hình virus hiện nay ở Thành phố. Chúng tôi mong nhận được ý kiến trao đổi và bàn bạc của tất cả các bạn đồng nghiệp cũng như của những ai quan tâm đến vấn đề này.(1)

NAV

(1) Mọi liên hệ xin theo địa chỉ :
Ban Dịch vụ Tin học - CESAIS 17 Phạm Ngọc Thạch Q.3