MỘT VÀI ĐẶC TRƯNG CỦA VIRUS DISK-KILLER

NGÔ ANH VŨ

Hiện nay trong làng tin học Thành phố đang xuất hiện một loại virus tương đối mới, đó là Virus "Disk Killer". Với sức phá hoại tàn khốc của mình, Virus này đã gây không ít nỗi lo sợ cho mọi người, từ đó dẫn đến một số ngộ nhận và cách chống lại không hiệu quả, tốn kém. Bài viết này chỉ nhằm nêu ra đặc trưng của virus và cách phòng chống.

SỰ RA ĐỜI

Version 1-0 ra đời vào ngày 1 tháng 4 năm 1989 do ORGE COMPUTER (theo bản quyền virus).

VIỆC LƯU TRÚ TRONG VÙNG NHỚ CỦA DISK-KILLER:

1. Tương tự như các B-Virus khác, Virus Disk-Killer cũng phải dọn cho mình một chỗ trong vùng nhớ khi máy đã nhiễm Virus được khởi động. Việc dọn chỗ được tiến hành tương tự như Brain. Virus được chia làm 2 phần: phần đầu và phần thân.

- Phần đầu: nằm ngay ở Boot sector (đối với đĩa mềm) hay Boot partition active (đối với đĩa cứng). Khi phần đầu được trao quyền điều khiển, nó sẽ tải phần thân và trao quyền điều khiển lại.

- Phần thân: Virus tiến hành chiếm 8Kb memo trên cùng để làm nơi "cư ngụ" của mình và đặt lại một số ngắt như int 8, int 13. Sau khi đặt lại, virus lại tải bằng Boot chuẩn vào, trao quyền cho nó.

2. Đặc biệt; Nếu máy bị Cold Boot, virus sẽ làm lại phần này.

LÂY LAN

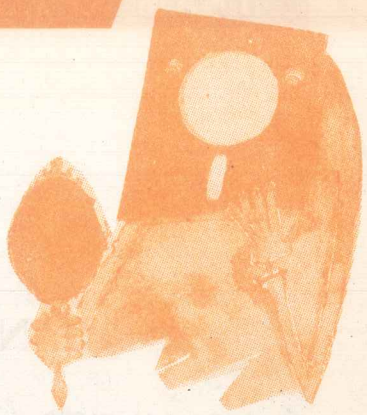
Mọi tác vụ đọc bảng FAT/DIRECTORY đều dẫn đến việc lây lan. Tất nhiên theo truyền thống của các B-virus trước, và bảo đảm tính duy nhất (đã nêu ra ở bài trước- PTKT số 2/1990) bằng cách kiểm tra giá trị ở W[ØE]=3CCBh. Cũng chính vì điều này, mọi chương trình Protect disk sẽ không còn hiệu quả vì cả Brain 9.2 lẫn Disk Killer đều kiểm tra W[E] = 1234, và vì vậy đây là một hướng phòng chống lâm vào ngõ cụt.

1. Đối với đĩa mềm

Tương tự như Brain, tuy nhiên có mở rộng việc lây lan cho mọi đĩa mềm bằng cách đưa vào BPB (Bios parameter boot).

- Đánh dấu các cluster trên đĩa chứa thân virus là cluster hỏng, số lượng cluster phụ thuộc vào loại đĩa.

2. Đối với đĩa cứng:



Không như một số tài liệu của Mc Afee công bố, Disk-Killer lây đĩa cứng không qua Boot Master mà qua Partition Boot Active. Bằng cách này, virus dễ qua mặt một số người quan tâm đến Boot Master. Thân virus không nằm trong cluster nào và FAT cũng không bị sửa đổi (vì khó mà xác định FAT là 12 hay 16 và định vị nó) mà nằm ở những sector hidden được đánh dấu.

CÁCH PHÁ HỦY ĐĨA

Các phá hoại đĩa của Disk-Killer mang tính "ngang tàng "với dòng công do bản quyền và câu thông báo "Don't power off or remove diskette while disk killer is processing".

Sau khi máy đã bị nhiễm 48 giờ (tính theo giờ máy đã chạy thực sự), virus sẽ tiến hành phá hủy đĩa.

Việc kiểm tra công tác đếm giờ do virus đảm nhiệm gồm 2 phần W[1FØh] và B[1F2]. Giá trị khởi đầu của W[1FØh] là Ø. Sau mỗi nhịp đồng hồ sẽ được tăng 1, khi tràn B[1F2] được tăng 1. Khi tràn ô tương ứng với 1 giờ chạy máy. Vậy nếu giá trị B[1F2] = 30h sẽ gây ra phá hủy.

Việc phá hủy chỉ đơn giản là sự sắp xếp loại thông tin trên đĩa theo một cách khác. Do đó DOS không thể kiểm soát nổi Disk một khi đã bị virus phá hủy. Các nội dung này có thể phục hồi nếu chúng ta chịu khó tuân theo qui định của virus, nghĩa là chịu khó ngồi chờ virus thực hiện hết nhiệm vụ của mình và chúc chúng ta may mắn bằng một câu thông báo "I wish you luck".

Và cũng thật may mắn, chúng ta có thể phục hồi lại đĩa sau khi bị phá hoại.

CÁCH PHONG CHỐNG

Hiện nay đã có một số nơi (trong và ngoài nước) đã chống được loại virus này. Tuy nhiên, cách xử sự ở các cơ quan khi phát hiện đều ở hai dạng:

- Hoặc phát hiện sự rối loạn của đĩa và tiến hành format đĩa.

- Bị virus phá hủy thông tin trên đĩa [1].

1. Đối với trường hợp sau này, nếu cần thiết phải "cứu" thông tin trên đĩa xin liên hệ với chúng tôi theo địa chỉ:
Trung tâm CESAIS
17 Phạm Ngọc Thạch, Quận 3, TP. HCM
Trường hợp đầu: Dùng các phần mềm để chữa trị như MEDICINE 1.02 hay AVT 1.07.