B-virus

Bởi:
Khoa CNTT ĐHSP KT Hưng Yên

Cấu trúc đĩa cứng

Cấu trúc vật lý

- Track
- Side
- Cylinder
- Sector

Cấu trúc logic

- Boot sector
- FAT
- Root directory
- Bảng Partition

Dịch vụ truy nhập đĩa

- Mức BIOS (basic Input/Output System)
- Mức DOS

Phân tích B-virus

Đặc điểm

- B-virus triển khai kẽ hở của hệ thống để chiếm quyền điều khiển.
- Nạp trước hệ điều hành
- Không phụ thuộc vào môi trường

Cấu trúc của một b-virus thường bao gồm hai phần: phần cài đặt và phần thân

Phân loại

sb-virus:

B-virus

- Chỉ dùng một sector thay chỗ boot record
- Cất boot record vào các sector cuối trong Root Directory hoặc trong đĩa mềm hoặc lưu trong các sector của track 0 trong đĩa cứng.

db-virus

- Chương trình chia làm hai phần, dùng nhiều sector

Các yêu cầu của một B-virus

- Tính tồn tại duy nhất
- Tính lưu trú
- Tính lây lan
- Tính phá hoại
- Tính gây nhiễm và ngụy trang
- Tính tương thích

Nguyên tắc hoạt động

Do chỉ được trao quyền điều khiển một lần khi boot máy, do đó b-virus phải tìm mọi cách để tồn tại và hoạt động giống như một chương trình thường trú. Chương trình thường gồm hai phần, một phần nằm tại boot record, phần còn lại nằm trên đĩa và được tải vào bộ nhớ khi virus được kích hoạt.

Phần install

Đã tồn tại trong bộ nhớ chưa →

↓

Đọc phần thân (db-virus)

↓

Nạp chương trình và lưu trú

↓

Chiếm các ngắt cứng (13, 8, 9)

↓

Trả boot sector cũ

B-virus

↓

JMP FAR 0:07C00

Phần thân

- Phần lây lan
- Phần phá hoại
- Phần dữ liệu
- Phần boot record

Kỹ thuật lây lan

Đọc/Ghi →

↓

Đọc boot sector

↓

Đã nhiễm →

↓

Ghi boot sector của virus

↓

Ghi phần thân vào một vùng xác định →

(chi tiết xem [16])

Phòng chống và diệt B-virus

Phòng

Chúng ta nên cài đặt và sử dụng các chương trình phòng chống virus, đặc biệt cần nâng cao ý thức cảnh giác trong quá trình sử dụng máy tính chẳng hạn như luôn thực hiện việc sao lưu dữ liệu, kiểm tra đĩa mềm trước khi đưa vào máy, bật nấc chống ghi trên đĩa mềm, …

Phát hiện

Việc phát hiện b-virus có thể tiến hành theo hai cách dựa vào đặc điểm của b-virus đó là kiểm tra virus trong vùng nhớ và trên đĩa.

Trong vùng nhớ

B-virus tồn tại trong vùng nhớ cao, việc phát hiện có thể qua các bước sau:

- So sánh tổng số vùng nhớ
- Dò tìm đoạn mã xác định của chương trình virus
- Có thể vô hiệu hoá virus bằng cách dành lại ngắt 013 cũ.
- Vô hiệu hoá virus và khởi động lại máy là phương pháp tốt nhất hiện nay

Trên đĩa

Việc dò tìm trên đĩa phải thực hiện sau khi kiểm tra vùng nhớ không phát hiện được virus. Việc phát hiện virus trên đĩa có thể tiến hành bằng nhiều cách:

- Dò tìm đoạn mã
- Kiểm tra key value

Gỡ bỏ B-virus

Sửa lại boot record theo các bước:

- Tìm nơi virus cất dấu boot sector
- Đọc và kiểm tra boot sector/partition trên cơ sở bảng tham số BPB (Bios Parameter Block) và dấu hiệu nhận dạng đĩa
- Khôi phục boot sector