CÁC CÁCH ĐƠN GIẢN ĐỂ PHÒNG TRÁNH VIRUS LÂY QUA USB

Nếu bạ

Nếu bạn bỏ thói quen bấm đúp chuột hay bấm phải chuột vào biểu tượng ổ USB, thiết lập cơ chế bỏ chạy tự động (Autorun), cho hiển thị tập tin ẩn và đuôi file... thì sẽ không bị nhiễm virus lây trên thiết bị phổ thông này.

1. Cho hiển thị file ẩn và đuôi file

Trước khi cắm ổ USB bất kỳ vào máy, bạn hãy mở Windows Explorer. Ở menu Tools > tìm dòng Folder Options. Nếu không có mục này thì nghĩa là máy của bạn đang hoặc từng bị virus và bạn cần dùng những chương trình diệt virus mới nhất để diệt cho sạch sẽ, và áp dụng các giải pháp khắc phục tác hại của virus lây qua USB.

Trong hộp thoại Folder Options vừa mở ra, bạn nhấn vào tab View, tìm các dòng sau và bấm/ huỷ bấm dấu kiểm của những dòng tương ứng:

Tích chọn Show hidden files and folders
Bỏ dấu kiểm Hide extensions for know file types
Bỏ dấu kiểm Hide protected operating system files (Recommended)

Mục đích của thao tác này là để hiển thị virus cố tình giấu mặt trong ổ USB bằng cách tự đặt cho nó thuộc tính "ẩn" (Hidden và System), và hiển thị những virus giả danh (có biểu tượng giống file word hay giống biểu tượng folder, nhưng thực ra nó là file thực thi *.EXE) để khỏi vô tình bấm nhầm khiến nó hoạt động.

Nếu bạn không cho hiển thị đuôi file thì bạn sẽ không thể phân biệt được đâu là tài liệu thật, đâu là virus vì chúng đều có tên giống nhau, biểu tượng (icon) giống nhau, và chỉ khác nhau duy nhất phần đuôi (mở rộng) file (*.EXE và *.DOC chẳng hạn). Trong khi đó, để "tiện dụng" theo mặc định của Microsoft, phần đuôi file này không được hiển thị nên người dùng rất dễ nhầm lẫn.

Khi thấy file EXE có biểu tượng giống Word, giống Folder và có tên file giống tài liệu của bạn thì hãy xoá thẳng tay và không được bấm đúp vào đó để xem.

2. Bỏ thói quen bấm đúp chuột trái và bấm chuột phải

Đa số người dùng đều có thói quen cắm ổ USB vào máy, mở Explorer nhấn đúp chuột trái vào biểu tượng ổ USB trong My Computer để mở.

Nhưng rất nhiều virus có đặc tính tạo ra một file "Autorun.inf" ở ngay bên ngoài ổ USB, có thể ẩn hoặc không. File này về bản chất không xấu, nó được Windows cho tự động chạy một phần mềm quy định trong nội dung của file "Autorun" để tạo ra sự thuận tiện cho người dùng. Virus lại lợi dụng file đó để tự động kích hoạt nên nếu thấy sự xuất hiện của file đó trên ổ USB hoặc bên ngoài cùng ổ cứng (C:\; D:\; E:\) nghĩa là ổ USB hoặc máy tính của bạn đã có virus.

Kể cả bạn đã thận trọng bấm chuột phải vào biểu tượng ổ USB và chọn Explorer hoặc bất kỳ một mục gì khác để mở ổ USB từ menu bật ra, bạn vẫn bị virus. Bởi virus đã chỉnh sửa file Autorun.inf, và thông qua đó đã chỉnh sửa luôn cả menu bật ra khi bạn bấm chuột phải để khi người dùng chọn Explorer, virus vẫn được kích hoạt.

Do đó, hãy mở cửa sổ My computer bằng cách bấm nút Windows-E, và bấm đơn (một lần trên chuột trái) vào hình ổ USB ở bên trái trong cây thư mục (Folder tree). Hoặc bấm vào nút sổ xuống (drop-down) của Address bar, và chọn ổ USB trong danh sách ổ đĩa xổ xuống đó. Bạn vẫn mở được ổ USB ngay cả khi USB có virus, còn virus thì không thể vào được máy nếu bạn thận trọng làm như vậy.

3. Vô hiệu hoá tính năng Autorun

Mặc dù đã "cảnh giác" để mở USB như mục 2, nhưng đôi khi người dùng vẫn cứ nhầm lẫn. Vì vậy, tốt hơn hết là vô hiệu hóa Autorun bằng cách sau:

Tạo một giá trị DWORD với tên "NoDriveTypeAutorun" tại khóa HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer của registry rồi đặt giá trị theo bảng dưới đây.

Hệ 10
Ý nghĩa

0 x 1
1
Vô hiệu hóa Autorun của các ổ đĩa chưa biết kiểu

0 x 4
4
Vô hiệu hóa Autorun của các ổ đĩa tháo lắp được

0 x 8
8
Vô hiệu hóa Autorun của các ổ đĩa cố định

0 x 10
16
Vô hiệu hóa Autorun của các ổ đĩa mạng

0 x 20
32
Vô hiệu hóa Autorun của các ổ đĩa CD-ROM

0 x 40
64
Vô hiệu hóa Autorun của các đĩa RAM

0 x 80
128
Vô hiệu hóa Autorun của các ổ đĩa chưa biết kiểu

0 x FF
255
Vô hiệu hóa Autorun của các ổ đĩa

Người dùng nên mở phần mềm ra trước rồi gọi tập tin ra sau

Theo đó, nếu muốn vô hiệu hóa tính năng Autorun của tất cả các ổ đĩa trừ đĩa CD ROM, bạn tính 1+4+8+16+64+128 = 221 (bỏ giá trị 32 cho CD ROM), đổi ra hệ cơ số 16 được DD (sử dụng Calculator của Windows) rồi nhập giá trị DD cho "NoDriveTypeAutorun". Để vô hiệu hóa tính năng Autorun của tất cả mọi loại đĩa, bạn nhập FF. Sau đó khởi động lại máy để thay đổi có hiệu lực.

4. Dùng menu Open
Điều đơn giản và an toàn nhất là để mở một file tài liệu bất kỳ (Word, Excel, Access, AutoCAD...) hãy mở phần mềm ra trước, rồi bấm nút menu File/ Open để mở tài liệu vì mọi phần mềm đều có chế độ lọc bỏ những file không phải là tài liệu chính thức của nó.

Đừng tiện lợi hoá bằng cách trông thấy tài liệu là ngay lập tức bấm đúp chuột để mở.