HƯỚNG DẪN CÁCH PHÒNG CHỐNG VIRUS

Cách đây vài năm , các virus máy tính chủ yếu lây nhiễm với mục đích là phá hoại dữ liệu trên con PC của bạn chủ yếu là phá các file .exe hay .dll … thì ngày nay mấy loại virus đấy hầu như bị tuyệt chủng mà thay vào đó là các con trojan hay malware lây lan nhanh và hiệu quả hơn nhằm mục đích đánh cắp thông tin cá nhân hay đơn giản là gây khó chịu cho bạn trong việc sử dụng windows .

Những loại virus này ngày càng tinh vi hơn trong cách lây lan mà nhiều bạn chưa có kinh nghiệm dễ mắc phải những cái bẫy đơn giản mà vô cùng hiệu quả của chúng .

Bạn sở hữu 1 phần mềm diệt virus mà bạn vô cùng tin tưởng , tự tin xông pha trong thế giới internet bất chấp nó có chứa virus hay không .Tôi cho rằng đó là cách hiểu tiêu cực , không phải phần mềm nào cũng hoàn hảo , có thể bảo vệ chiếc PC của bạn 1 cách tuyệt đối .Tôi không bao giờ tin tưởng và giao phó hoàn toàn sinh mệnh của PC cho nó , cách phòng chống tốt nhất là chính ở cách bạn sử dụng máy tính hiệu quả như thế nào và bạn am hiểu về các loại Virus tới đâu để mà Phòng chống . Nhân đây tôi sẽ hướng dẫn 1 số cách Phòng chống đơn giản để hạn chế bớt Virus xâm nhập vào máy tính của Bạn .

1 . **Dùng tường lửa (Firewall) :** để chặn các kết nối không mong muốn từ Internet với máy tính của bạn . Vì thế , bạn nên để mặc định , từ chối tất cả các kết nối bên ngoài , chỉ cho phép các dịch vụ (service) mà bạn muốn sử dụng .

Phần mềm tường lửa thì có rất nhiều loại phần mềm nhưng nếu bạn hiện tại chưa có phần mềm nào thì bạn cũng có thể dùng tường lửa mặc định của Microsoft Windows .

Đầu tiên để sử dụng được Phần mềm tường lửa của Microsoft Windows thì bạn phải bật dịch vụ này lên . Bạn làm như sau :

Bạn vào Start , Run , gõ services.msc . Sau đó , Bạn tìm Dịch vụ nào có tên là Windows Firewall/Internet Connection Sharing (ICS) . Bạn phải chuột vào Dịch vụ đó và chọn Start để bật tường lửa này lên .

Nếu Bạn muốn thay đổi 1 số thông số của phần mềm này thì bạn chỉ cần phải chuột vào biểu tượng Card mạng (Hai hình máy tính lồng vào nhau ở góc phải màn hình) và chọn Change Windows Firewall Settings .

2 . **Sử dụng chính sách mật khẩu phức tạp :** Một mật khẩu được đánh giá là phức tạp khi mật khẩu đó có cả chữ , cả số , cả ký tự đặc biệt và phải dài hơn 7 kí tự .

Và bạn không nên để mật khẩu trắng , nên Set Password User của Microsoft Windows khi vừa nhận máy tính .

Thì khi đó tin tặc (hacker) mới khó có thể dò ra mật khẩu của Bạn .

Để cài đặt mật khẩu cho một User bạn phải làm theo các Bước sau :

Đầu tiên , bạn phải tắt chế độ Welcome Screen . Vì khi bạn sử dụng ở chế độ này thì tin tặc cũng đã biết được 50% thông tin và thông tin đó là tên Account mà Bạn login vào máy tính của bạn .

Để tắt chế độ Welcome Screen này bạn phải vào Start \ vào Settings \ Phải chuột vào Control Panel và chọn Open \ vào User Accounts (như hình bên dưới) .

Bạn nhấn tiếp vào Switch to Classic View để hiển thị tất cả các chương trình bên trong Control Panel .

Vào tiếp User Accounts .

Bạn nhấn vào tiếp Change the way users log on or off (thay đổi cách logon vào máy tính) .

Tắt dấu check ở mục Use the Welcome screen (Tắt / mở chế độ Welcome Screen) .

Và chọn Apply Options .

Cách 1 : Cách đổi Password này sẽ không làm ảnh hưởng đến dữ liệu mã hóa .

Bạn nhấn Ctrl+Alt+Delete . Sau đó , Bạn chọn Change Password… (Để thay đổi Password Logon vào máy tính) .

Bạn nên Đánh Password cũ vào và Password mới vào , rồi nhấn OK . Sau khi nhấn OK là Bạn đã thay đổi Password xong .

Cách thay đổi Password này là tuyệt đối An toàn đối với Dữ liệu của Bạn , vì nó có xác nhận lại Password cũ của Bạn .

Cách 2 : Cách này An toàn khi Bạn không có mã hóa dữ liệu . Nếu có mã hóa dữ liệu thì Bạn sẽ bị mất dữ liệu mà bạn đã mã hóa .

Đầu tiên , Bạn muốn biết User bạn đang Login là gì , bạn chọn vào Start , sau phần Log Off là tên User bạn đang Login .

Sau đó , Bạn phải chuột vào My Computer , sau đó chọn Manage , vào Local Users and Groups . Chọn tiếp vào Users . Phải chuột vào User mà bạn đang sử dụng chọn Set Password… . Chọn Proceed để đồng ý cài Password cho User .

Bạn đánh vào Password mới , sau đó nhấn OK là bạn đã hoàn tất việc đổi Password của bạn . Nhưng tôi khuyên bạn nên sử dụng cách 1 vì cách 1 an toàn dữ liệu của Bạn hơn .

3 . **Vô hiệu hóa chức năng AutoPlay của USB :**

Để tránh bị nhiễm virus khi bạn cắm USB vào máy tính .

Vì khi bạn cắm USB vào máy tính thì chức năng AutoPlay tự động kích hoạt , khi chức năng này được kích hoạt thì Virus từ USB sẽ tự động vào máy tính của Bạn .

Vì vậy , bạn phải làm theo các bước sau để tắt chế độ AutoPlay của tất cả các ổ đĩa trong máy tính của Bạn .

Các bước thực hiện như sau :

Bước 1 : Vào Start , Run , gõ : **gpedit.msc** và nhấn Enter để vào chương trình Group Policy .

Bước 2 :

Bạn nhấn vào để mở 2 mục :

+ Computer Configuration \ vào tiếp Administrative Templates \ vào tiếp System .

+ User Configuration \ vào tiếp Administrative Templates \ vào tiếp System .

Bạn chọn Turn off Autoplay , chọn Enable , chọn All Drives và nhấn OK .

Sau khi bạn nhấn OK , bạn Restart lại máy tính để việc chỉnh sửa này được áp dụng .

Các bước làm bạn xem hình bên dưới . Sau khi bạn làm xong bước này thì bạn đã hạn chế phần nào Virus từ USB lây lan sang máy tính của Bạn . Đây mới chỉ là bước đầu để phòng chống Virus lây lan qua USB .

Để hiểu rõ hơn về cách lây nhiễm và cách Phòng chống nâng cao , bạn tham khảo cách dưới đây :

Virus phát tán qua ổ USB như thế nào?

Cơ chế thứ nhất - Autorun (tự chạy)

Nếu bạn đã từng đẩy một đĩa CD vào khay và chờ 1 chút , 1 chương trình cài đặt hiện lên , mọi thứ bắt đầu . Nếu tinh ý bạn sẽ thấy là có một cơ chế tự động (Autorun) đằng sau đó , và chắc chắn ít nhiều đã có một chương trình nào đó được thực thi . Chuyện gì xảy ra nếu chương trình vừa chạy này là một chương trình xấu , chứa những dòng mã hiểm độc nhằm hủy hoại máy tính của bạn ? .

Cũng tương tự như ổ CD-ROM của bạn , tất cả các ổ đĩa khác bao gồm đĩa cứng , đĩa mềm và USB Flash Drive , đều có thể ẩn chứa khả năng Autorun này . Cũng không thể nói rằng Autorun là một tính năng xấu , nhưng đây là một lỗ hổng cho những kẻ cơ hội khai thác và cũng là cơ chế lây lan cơ bản của hầu hết các virus USB . Bạn sẽ phải dè chừng nó .

Cơ chế thứ hai - Fake Icon (giả biểu tượng)

Virus máy tính do con người viết nên và nó có tính chất tự nhân bản , để hoạt động được đòi hỏi phải có môi trường và những điều kiện cụ thể (trong trường hợp trên thì cơ chế Autorun đã thực thi virus) . Còn trường hợp phổ biến thứ hai , một "con" virus (dưới dạng một file .exe) giả dạng làm một thư mục hay file quen thuộc của bạn. Virus ngụy trang bằng cách mang trong mình icon của folder/file y hệt như icon thật, điều đó làm bạn dễ nhầm lẫn double click vào icon này. Sau khi bạn click, chẳng có thư mục hay file nào được mở ra cả, tất cả những gì bạn làm là đã thực thi 1 file .exe - vậy là virus đã được kích hoạt, máy của bạn bị nhiễm virus!.

Cách Phòng Chống virus USB

Các động tác cơ bản

Trước khi bắt đầu với đám virus USB, chúng ta nên có một số thao tác đón đầu trước để sau đó làm việc dễ dàng hơn :

Thay đổi một số thuộc tính cơ bản

Vào My Computer, chọn menu Tool > Folder Options…

Trong cửa sổ Folder Options chọn tab View, cuộn thanh cuộn xuống 1 chút và cấu hình như sau:

Chọn *Show hidden files and folders* để hiển thị các file ẩn (hidden file), bởi vì lẽ dĩ nhiên các virus tự ẩn mình đi.

Bỏ chọn *Hide extensions for known file types* để hiển thị đuôi (vd *.exe *.doc *.txt…) cho tất cả các file.

Bỏ chọn *Hide protected operating system files* để hiển thị những file hệ thống quan trọng. Bạn sẽ thấy là mục này được ghi chú là Recommended, tức là khuyến cáo nên để ẩn chứ không nên cho hiện hết ra. Cũng đúng thôi, vì sau khi chọn mục này, bạn sẽ thấy xuất hiện nhiều file và thư mục hệ thống lờ mờ trên khắp các ổ cứng của mình, nếu không may xóa phải các file này thì rất có thể máy của bạn sẽ gặp rắc rối lớn. Tuy nhiên các virus cũng tự ngụy trang mình bằng cách khoác lên mình chiếc "áo" làm file hệ thống, để nhìn thấy chúng bạn phải bỏ chọn mục này. Nếu ổ USB có virus thì thực hiện như hình 4 để xóa các file nguy hiểm. Nhớ: không xóa bất kỳ file nào loại này mà bạn chưa chắc chắn là virus.

Cách chống virus USB lây sang máy tính

Không cho virus tạo file **Autorun.inf , Autorun.ini** trong ổ đĩa (cả ổ cứng và ổ USB):

Có thể có nhiều cách chống được loại virus này. Tuy nhiên, cách đơn giản mà không cần công cụ gì giúp ổ cứng của bạn hạn chế bị virus USB tấn công và phát tán là tạo một file Autorun.inf , **Autorun.ini** (không có nội dung gì) trong thư mục gốc của ổ đĩa, không phân quyền cho bất kỳ user nào có thể thay đổi file đó để virus không tạo được file Autorun nữa. Cách làm như sau:

Ổ cứng của bạn phải được định dạng theo NTFS (Nếu là FAT32 thì không phân quyền cho file được) .

Mở Explorer rồi vào menu Tools \ Folder Options \ View, kéo xuống dưới rồi bỏ chọn mục Use simple file sharing --> OK .

Tạo một file Autorun.inf , **Autorun.ini** (không có nội dung), Click chuột phải chọn Properties \ Security \ Advanced, tại bảng Permissions hãy Remove hết tất

cả các user có trong danh sách rồi chọn OK --> Yes, trở về mục Security sẽ thấy danh sách các user trống rỗng là được, sau đó chọn OK.

Sau khi thao tác như trên, nếu không xóa được file Autorun.inf , **Autorun.ini** là bạn đã làm đúng.

Với những gì đã làm kết hợp với việc thực hiện "Các bước truy xuất ổ đĩa an toàn" như hình vẽ ở dưới thì bạn không lo bị nhiễm virus USB nữa.

Cuối cùng là bạn phải Restart lại máy để bước 1 có hiệu lực, cách này không hẳn là phòng chống được virus USB 100%, nhưng cũng hạn chế tối đa được loại virus lây qua ổ USB này.

Cách Convert ổ đĩa từ FAT sang NTFS: Chọn Start -> Run -> gõ lệnh cmd -> OK. Tại cửa sổ lệnh bạn gõ lệnh để convert theo cú pháp: CONVERT volume /FS:NTFS /V /X . Ví dụ muốn convert ổ F, bạn gõ lệnh như sau:

Convert f: /FS:NTFS **/X /V**

Một số lưu ý :

Dấu hiệu nhận biết khả năng ổ đĩa bị nhiễm virus USB (kích chuột phải vào biểu tượng ổ đĩa) :

Hình 1. Bình thường Hình 2. Bị nhiễm Hình 3. Bị nhiễm

Nếu kích đúp chuột vào biểu tượng ổ đĩa thì: Hình 1, 99% sẽ mở ra thư mục gốc. Hình 2 và 3 (ổ đã bị nhiễm virus USB), 100% sẽ kích hoạt nội dung các câu lệnh trong file Autorun.inf , Autorun.ini .

Cách truy cập ổ đĩa nhằm khống chế sự kích hoạt file Autorun.inf , Autorun.ini

Vào My Computer, nhấn vào biểu tượng Folders sẽ thấy xuất hiện List các Folders bên trái, muốn mở ổ đĩa nào chỉ cần bấm chuột vào biểu tượng ổ đĩa đó. Ở cửa sổ phải sẽ xuất hiện các file và thư mục trong ổ đĩa, lúc này bạn có thể truy cập vào các file và thư mục mà không sợ kích hoạt file Autorun.inf , Autorun.ini .

Các bước truy xuất ổ đĩa an toàn

Cách chống* Fake *Icon :

Mỗi chương trình, mỗi loại file mang trên mình một biểu tượng. Lợi dụng điều này mà các loại virus USB mạo danh để hòng lừa gạt người dùng kích hoạt chúng. Vấn đề là nếu một chương trình virus mang icon của một folder/file khác, thật khó phân biệt và người dùng dễ nhầm lẫn double click thực thi chương trình này. Mặc định, Windows giấu đi phần đuôi của những chương trình, file đã biết. Vd: file

STARTUP.exe được hiển thị trong My Computer chỉ còn là STARTUP. Nếu file này mang icon của một thư mục, thật khó phân biệt. Chẳng hạn như ở hình dưới, bạn cứ ngỡ STARTUP là một thư mục:

Phân biệt cơ chế Fake Icon của virus

Nhưng nếu bạn cho hiện hết đuôi các file ra (xem lại Các động tác cơ bản), thì các file này "lòi đuôi" ra ngay là file thực thi.

Bạn cũng có thể xem file ở dạng Details (chọn menu Views > Details), lúc này hãy chú ý đến sự khác biệt giữa một thư mục (folder) và ứng dụng (application):

- ✓ Ở cột Type, ứng dụng được gọi là Application còn thư mục là File Folder.
- ✓ Ở cột Size, ứng dụng có size còn thư mục thì không.

Cần lưu ý, các virus còn giả danh các file thường dùng, như file text (.txt), file word document (.doc), file ảnh (.jpg) v.v.

Như vậy, để kiểm tra xem USB Drive có nhiễm virus loại này không, bạn có thể truy cập vào USB, bật chế độ hiện hết các đuôi file và chú ý đến các đuôi .exe. Hoặc cũng có thể view ở chế độ details và chú ý đến các Application. Nếu gặp các virus loại này? Hãy xóa thẳng tay.

Bây giờ bạn thử dạo qua một vòng ổ cứng của mình và một vài thư mục con để kiểm tra xem máy đã bị nhiễm virus loại này chưa.

4 . **User bạn sử dụng bạn không nên gắn cho toàn quyền :**

Các bạn nên tạo 1 User để sử dụng thường xuyên trong công việc và hạ quyền User đó xuống không cho cài đặt hay thay đổi gì có liên quan đến hệ thống .

Bạn để dự phòng 1 User có toàn quyền để khi nào cần cài hay cần thay đổi thì bạn sử dụng User này .

Khi tin tặc hay Virus có xâm nhập vào máy tính của bạn với User hiện tại thì cũng không có quyền gì cả để có thể thực thi đoạn mã độc hay tin tặc có thể chiếm quyền điều khiển của Bạn được .

5 . **Tắt chức năng chia sẻ file :** Nếu cần thiết phải chia sẻ file thì bạn nên sử dụng mật khẩu để hạn chế truy cập. Ngoài ra, bạn cũng nên tắt chức năng truy cập "mờ ám" vào các folder chia sẻ. Chỉ cho phép những người nào biết tên truy cập và mật khẩu của file chia sẻ.

6 . **Tắt hoặc gỡ các dịch vụ không cần thiết :** Theo mặc định, nhiều hệ điều hành tự động cài các dịch vụ phụ trợ vốn chẳng cần thiết. Những dịch vụ này hóa ra lại là các "ngọn nguồn" gây ra những vụ tấn công nguy hiểm. Thế nên, bạn nên gỡ bỏ chúng trước khi gặp hạn.

7 . Thường xuyên nâng cấp bản vá an ninh, đặc biệt với những máy tính sử dụng các dịch vụ công cộng.

8 . Cấu hình cho máy chủ e-mail để ngăn chặn hoặc xóa những e-mail có chứa những file đính kèm đáng ngờ.

9 . Nhanh chóng "cô lập" những máy tính đã bị nhiễm virus để tránh lây lan sang các máy khác.

10 . Lưu ý không nên mở những file đính kèm không đáng tin cậy. Và, cũng không nên chạy phần mềm download từ Internet mà chưa qua quá trình quét virus.

11 . Nếu chức năng Bluetooth của laptop mà không cần thiết thì nên tắt bỏ chúng. Nếu cần sử dụng thì nên cài đạt ở chế độ Ẩn để không bị các thiết bị khác dò thấy. Ngoài ra, người dùng nên yêu cầu xác thực trước khi kết nối Bluetooth với máy tính.

12 .Khi bạn chat Yahoo bạn không nên tò mò nhấn vào những Link không rõ nguồn gốc

Đây hình ví dụ minh họa 1 trường hợp tin nhắn offline bị virus gửi cho Bạn .

13 .Khi truy cập Internet : Không nên vào các trang web không lành mạnh , các trang web có chứa các công cụ crack phần mềm rất dễ bị virus .

14 .Bạn không nến nhấn vào bất kỳ 1 Link cảnh báo có Virus nào mở bằng Internet Explorer , Link cảnh báo này sẽ báo là máy bạn đã bị nhiễm Virus .

Lúc này Bạn nên bình tĩnh , đừng nhấn vào Link đó (Virus thường lừa bạn nhấn vào Link này để Download Tools diệt Virus) , sau khi bạn nhấn sau thì bạn sẽ bị nhiễm Virus luôn .

Để cho chắc chắn , Bạn nên dùng chương trình quét Virus của Mình đang sử dụng để kiểm tra lại xem có nhiễm Virus hay không nhé .

15 .Bạn không nên Load về bất cứ 1 chương trình quét virus nào mà không tin cậy . Không nên quét Virus theo đường quét Virus Online .

Các chương trình Virus tin cậy như : Symantec , Kaspersky , Bkav , Bitdefender , Nod32 , Mcafee , Panda Antivirus , ...

Nói tóm lại là không nên cài bất kỳ chương trình nào mà không biết nguồn gốc có tin cậy được hay không . Khi cài vậy sẽ rất dễ bị nhiễm Virus .

Chúc các Bạn Phòng chống Virus một cách hiệu quả .