HƯỚNG DẪN DIỆT VIRUS CHO MÁY TÍNH

Thời đại công nghệ số mang đến cho chúng ta vô vàn những tiện ích, những điều mới lạ, những phần cứng, phần mềm khác nhau mà đôi khi chính những người sử dụng lâu năm hay các chuyên viên công nghệ cũng chưa kịp nắm bắt hết những thay đổi đó.

Chính từ những thay đổi nhanh chóng muốn tạo ra nhiều cái mới lạ hơn nên việc đi kèm với những thiếu sót, tạo nên những lổ hỗng trong các dữ liệu phần mềm là không thể tránh khỏi. Chúng vô tình giúp cho một "lực lượng" phần tử xấu tìm cách xâm nhập trái phép để gây hại cho chúng ta bất cứ lúc nào. Những phần tử này được giới công nghệ gọi với cái tên quen thuộc là "Hacker" (tin tặc), và công cụ để họ thực hiện việc xâm nhập trái phép chính là việc tạo ra các dòng virus khác nhau và ngày một nguy hiểm.

Virus xuất phát từ các phần mềm độc hại, nó là một loại phần mềm hệ thống do các tin tặc hay những người có chút ít kiến thức về lập trình hệ thống thích trêu đùa người khác tạo ra nhằm gây hại cho các máy tính. Tùy theo cách thức, mục đích mà tin tặc sử dụng, các loại virus sẽ có mức độ nguy hiểm khác nhau, từ việc chỉ hiển thị các cửa sổ cảnh báo "giả" y chang như của hệ điều hành mang theo thông điệp hù dọa tới việc tấn công chiếm quyền

kiểm soát máy tính và lây lan sang các máy tính khác. Hiện nay có các loại virus bao gồm worm, trojan, spyware, adware, keyloger, backdoor, rootkit…(ở đây tôi không đề cập đến định nghĩa các loại virus).

Đôi khi người dùng có kinh nghiệm thực sự cũng không thể nhận ra một máy tính bị tiêm nhiễm virus thực sự hay không vì chúng có thể ẩn náu trong các file thông thường hoặc như các file chuẩn.

Vì vậy, cách duy nhất để phòng chống để dữ liệu tránh bị các phần mềm độc hại xâm nhập là bạn có thể dựa vào một trong các triệu chứng sau, đồng thời bạn sẽ được hướng dẫn một số bước cơ bản để bạn tạm thời xử lý sự cố khi laptop đã nhiễm virus.

1. **Các triệu chứng thường gặp khi laptop bị nhiễm virus:**

a/ Triệu chứng dễ gặp nhất với các bạn khi sử dụng máy tính nói chung và laptop nói riêng là khi laptop bạn đột nhiên không thể kết nối được Internet như bình thường, thậm chí ngay cả khi bạn đã xử lý hết virus trong máy tính nhưng bạn vẫn không thể kết nối lại được. Bạn sẽ làm gì? Format lại ổ cứng và chịu cảnh mất mát đi một số phần mềm mà lâu nay vẫn sử dụng trong khi không tìm ra được nguồn cài đặt lại?

b/ Nếu bạn vẫn kết nối được Internet bình thường, bỗng dưng các pop-up quảng cáo lạ tự động bật lên khi bạn chưa mở trình duyệt hoặc khi bạn muốn vào một trang web quen thuộc thì lại không thể vào được trang web đó mà bị chuyển sang một trang web khác.

c/ Nguy hiểm hơn là xuất hiện luôn một pop-up cảnh báo "Máy tính của bạn đã bị nhiễm virus" hoặc có hàng chục, hàng trăm tab bật lên cùng một lúc gây khó chịu hoặc thậm chí máy tính bạn bị treo ngay tức khắc. Đó chính là lúc máy tính bạn đã bị nhiễm virus.

d/ Một khả năng để các hacker lừa bạn và chiếm quyền điều khiển máy tính của bạn là ngụy trang dưới dạng một "phần mềm bảo mật giả" (phần mềm "Fake" Anti-virus) mà ngay chính bạn cũng chưa hề cài đặt phần mềm đó. Hiện tượng bạn gặp phải chính là một cảnh báo "giả" bật lên thông báo rằng "Máy tính của bạn đang nhiễm virus" và yêu cầu bạn tải bản cập

nhật (update) của phần mềm "giả" này về để cài đặt. Thủ phạm sử dụng phương thức tấn công, cài trojan, backdoor để khai thác thông tin người dùng từ việc người dùng tải về phần mềm hoặc lén lút cài đặt "phần mềm chống virus giả mạo" lên trên máy của bạn. Ngoài ra, bạn còn sẽ phải chịu thêm một tổn thất khác khi đăng ký và mất một khoản tiền thanh toán để tải công cụ này về diệt virus cho bạn. Và tất nhiên quá trình quét virus với phần mềm chống virus giả mạo này sẽ diễn ra rất nhanh vì thực sự nó chẳng làm bất cứ điều gì.

Nếu bạn là người không rành rọt về máy tính thì khả năng trên 90% sẽ đồng ý tải về, và lúc này bạn đã trở thành một "miếng mồi ngon" cho những tin tặc lấy được những thông tin cá nhân quan trọng, gây nguy hiểm cho chính bạn và những người thân xung quanh.

Các triệu chứng mất kết nối Internet, Popup quảng cáo và phần mềm diệt virus "giả mạo"

e/ Các trường hợp khác mà các bạn có thể nhận biết bằng mắt "thường":

* Các triệu chứng liên quan đến hệ điều hành:

- Không thể đăng nhập vào hệ điều hành, bạn vừa gõ password Windows xong thì lại bị thoát trở ra màn hình đăng nhập. (login/ logout) hoặc laptop không thể nạp được hệ điều hành khi bạn khởi động.

- Các trang quảng cáo hoặc các ảnh không mong muốn được hiển thị một cách bất ngờ dù bạn không duyệt web. (có khả năng máy tính bạn bị nhiễm Adware).

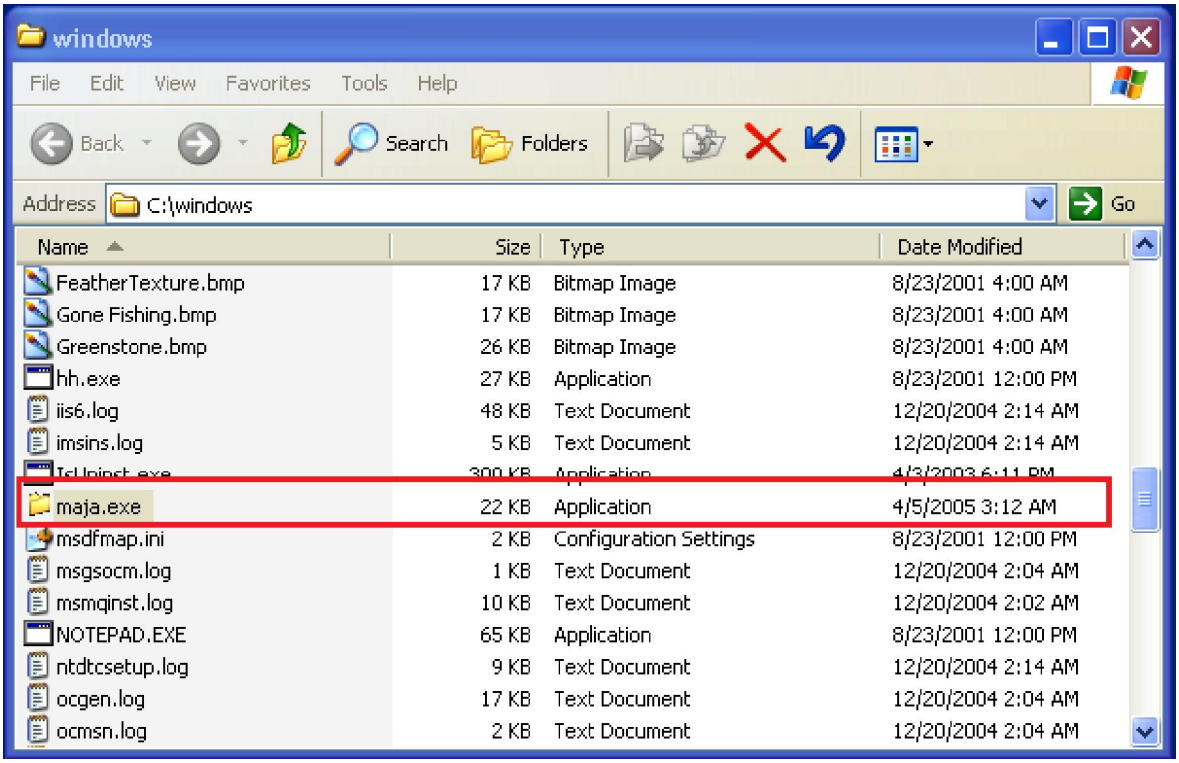
- Khi vừa đăng nhập vào Windows thì xuất hiện các đoạn nhạc hoặc âm thanh kèm theo những hình ảnh động có đuôi .gif được bật một cách ngẫu nhiên mà bạn không thể tắt được.

- Nếu máy tính bạn có bật tường lửa (Firewall) thì bạn sẽ liên tục nhận được các thông báo cảnh báo rằng có một số tiến trình nào đó đã có gắng thực hiện kết nối Internet đến một địa chỉ server ngoài mạng rất "lạ" mặc dù bạn không biết tiến trình đó là tiến trình gì và bạn cũng không chủ động khởi chạy nó.

- Các thư mục (folder) trong các ổ đĩa cứng tự động thay đổi biểu tượng (icon) khác thường. Ổ cứng gắn ngoài hoặc thanh nhớ USB gắn ngoài cũng bị thay đổi biểu tượng. Các file lạ tự động sinh ra khi bạn mở ổ đĩa USB.

- Hàng loạt các tập tin (file) xuất hiện với các tên tập tin rất "kỳ quái" giống như một chuỗi các ký tự chữ hoa, chữ thường và số xen lẫn nhau không thứ tự và khi chúng ta đọc lên cũng không có nghĩa. Dung lượng (size) của chúng cũng đồng nhất với nhau từ 1KB đến một vài KB.

- Xuất hiện các file có phần mở rộng .exe có tên trùng với tên các thư mục.



- Windows liên tục cảnh báo lỗi thiếu file hoặc không tìm thấy file khi khởi chạy các ứng dụng.

- Truy xuất tập tin, mở các chương trình ứng dụng chậm. Duyệt web chậm, nội dung các trang web hiển thị trên trình duyệt chậm.

- Các file và thư mục bị xóa hoặc bị thay đổi nội dung.

- Các thư mục và tập tin trong ổ đĩa của bạn bị "biến mất" một cách bất thường mà bạn không còn thấy được. Điều này là do một số loại virus làm ẩn đi tất cả các thư mục, tập tin gốc của Windows, sau đó thay thế bằng các thư mục, tập tin do chính nó tạo ra, khi người dùng click vào các thư mục, tập tin này thì vô tình kích hoạt virus "chạy" và phát tán sự lây nhiễm sang các ổ đĩa khác trong hệ thống.

- Không thể truy cập ổ đĩa cứng như thường lệ.

* Một số triệu chứng liên quan thông tin cá nhân:

- Người thân của bạn liên tục nhận được email từ hộp mail của bạn mà chính bạn không hề gửi các email đó.

- Liên tục mở hàng chục cửa sổ chat khi chạy ứng dụng Yahoo! Messenger.

- Kiểm tra hộp thư InBox, bạn thấy có rất nhiều các thông báo email gửi đến nhưng không có địa chỉ (address) hoặc tiêu đề (title) của người gửi, trong đó nội dung của mail có chứa các ký tự và link lạ và hướng dẫn bạn bấm vào để truy cập. *(Tuy vậy, bạn cũng nên xác nhận lại vì có một số trường hợp không phải bị gây ra bởi virus. Cho ví dụ, các thông báo bị tiêm nhiễm giả sử đến từ địa chỉ của bạn có thể lại được gửi từ một máy tính khác).*

2. Các phương pháp xử lý virus cơ bản khi bị nhiễm virus:

a/ Xử lý virus khi bị mất kết nối Internet:

Cách 1: Bỏ dấu kiểm tại mục proxy trong Internet Explorer. Một số loại virus sẽ trỏ các kết nối từ máy tính trực tiếp đến server của chúng, và bạn nên thực hiện bước này trước khi quét mã độc trên toàn bộ máy tính. Mở Internet Explorer và chọnTools -> Internet Options -> Connection Settings -> LAN Settings -> Bỏ dấu kiểm tại lựa chọn Proxy server -> OK.

Cách 2: Reset lại toàn bộ các thiết lập của trình duyệt, ở đây là Internet Explorer. Bạn làm theo các bước sau:

- Tắt tất cả các chương trình, ngoại trừ Internet Explorer.

- Nhấn tổ hợp phím WinKey + R, và gõ inetcpl.cpl.

- Tại thẻ Advanced Tab, ở phía dưới là lựa chọn Reset Internet Explorer Settings, nhấnReset -> OK, sau đó khởi động lại Internet Explorer.

Cách 3: Chỉnh lại file hosts như ban đầu. Thực chất, file này chứa tất cả các mapping – gọi đơn giản là "bản đồ" - của các website cho tới địa chỉ IP trên Internet, và Windows sử dụng file này để trỏ trình duyệt tới đúng địa chỉ website đó trên Internet. Cũng theo cách thức như vậy, virus đã len lỏi và thay đổi nội dung của file này, qua đó người sử dụng sẽ kết nối thẳng đến những địa chỉ độc hại đã được chuẩn bị sẵn. Các bạn hãy chỉnh sửa lại file hosts theo cách sau:

- Nhấn Windows + R và gõ%systemroot%\System32\drivers\etc vào ô Run.

- Đổi tên file hosts thành hosts.bak.

- Tạo mới một file text bằng Notepad với nội dung như sau:

Copyright (c) 1993-2009 Microsoft Corp.

#

This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

#

This file contains the mappings of IP addresses to host names. Each

entry should be kept on an individual line. The IP address should

be placed in the first column followed by the corresponding host name.

The IP address and the host name should be separated by at least one