TÌM HIỂU VỀ VIRUS, SPYWARE & ADWARE

Image not found or type unknown

Computer & Internet càng ngày càng phát triển một cách nhanh chóng vào đời sống chúng ta. Tuy nhiên có một số đề tài phổ biến không được rõ ràng cho lắm, có lẽ vì thiếu thông tin ... nên đôi khi chúng ta bị vài trở ngại nhỏ gặp phải. Trong bài sưu tầm này, tôi sẽ trình bày một cách ngắn gọn nhằm giúp quý vị hiểu biết thêm Computer & Internet.

1. Virus là gì?

Đây là một program được những tên hackers tạo ra để phá hoại computer chẳng hạn như PC cũng như server. Virus rất nguy hiểm, nó có thể làm ngưng sự hoạt động của chương trình nào đó, hoặc phá hủy đi memory của máy PC hoặc server.
Có loại virus chỉ làm thay đổi nhẹ màn hình (screen) nhằm mục đích "đùa giỡn", nhưng cũng có thứ ... phá huỷ toàn bộ tài liệu trong hard-disk mà nó tìm thấy. Một số loại virus khác lại còn có khả năng nằm chờ ... đến đúng ngày giờ đã định, nó mới phát tán và làm PC ngưng hoạt động.
Tùy theo khả năng hay phạm vi hoạt động, người ta có nhiều cách phân loại virus. Ở đây, tôi chỉ xin đưa ra vài loại mà chúng ta thường gặp nhất:

a) Virus qua e-mail:

Đại đa số các virus ngày nay thuộc vào lớp này. Lý do là virus có thể tự tìm ra danh sách các địa chỉ e-mail và tự nó gửi đi hàng loạt (mass mails) và có thể gây hại hàng triệu máy computers và làm tê liệt nhiều cơ quan trên toàn thế giới trong thời gian vô cùng ngắn.

Nhược điểm thứ nhất của loại virus này là chúng ta có thể loại bỏ dễ dàng vì nó được gửi dưới dạng đính kèm (attached mail). Do đó người dùng sẽ không bị nhiễm virus ... cho tới khi nào virus đính kèm được mở ra. Do đặc điểm này, các con virus thường được "trá hình" bởi các đề tài thật hấp dẫn như SEX, thể thao, miễm phí, hay dụ khị bán nhu liệu (software) với giá vô cùng rẻ...

Nhược điểm thứ nhì của loại virus này là self executable file, qua trung gian của những file có extension như: dll, exe, bat, vxd...

Cách tốt nhất là đừng bao giờ mở các file đính kèm trong e-mail qua những địa chỉ lạ, hoặc địa chỉ người quen mà chủ đề rất lạ, trừ khi quý vị biết rõ 100% là nó không chứa virus.

Lưu ý: Quý vị nào đang hiện dùng Outlook 95 hoặc cũ hơn, nên cần phải cẩn thận để tránh lầm tưởng một file có extension là .txt.exe và .txt (vì khi đó sự điều hành tự động dấu đi cái extention

“khỉ” exe). Thay vi nhìn thấy tên là “love.txt.exe” thì người đọc chỉ nhìn thấy “love.txt” và lầm rằng đó chỉ là ký tự nhưng kỳ thực nó là “con virus tình”.

b) Virus qua Internet:

Khác với loại qua e-mail, virus loại này thường ẩn mình trong các chương trình lậu (illegal) hay các chương trình miễn phí (freeware, shareware...). Thật ra không phải chương trình lậu hay chương trình miễn phí nào cũng có virus, nhưng một số tay hắc đạo (hacker) lợi dụng tâm lý “ham đồ rẻ, miễn phí, download lậu” này để bỏ virus vào.

Loại này thường hay nằm dưới dạng .exe và nhiều khi trong .zip file.

Đừng bao giờ nhấn nút OK mà không cần biết mình đã làm gì!!! Phải kiểm chứng những chú em này qua viện Pasteur?@#! (nhu liệu Anti-Virus) trước khi nhấn nút OK.

c) Các virus cổ điển:

Con Virus đầu tiên là phát minh của 1 thiếu niên ở Anh. Nó chỉ truyền được qua internet, CD/DVD ROM, ZIP/ZAP disk, hay băng từ... Con virus nổi tiếng trong lich sử computer loại này có tên là là Stealth. Nó có khả năng thay đổi ngay cả chức năng của BIOS. Ngày nay, Stealth vẫn còn nhưng đã được biến dạng (hiện đại hoá ... virus) thành một trong hai loại kể trên.

Cách phòng ngừa tốt nhất để tránh virus:

Cần một nhu liệu chống virus, hiện nay có hai nhà sản xuất nổi tiếng nhất đó là Norton và McAfee. Đôi khi mua với rebate và upgrade, quý vị cảm thấy không tốn xu-ten nào. Chỉ tốn tiền thuế, stamp, bìa thư ... mà thôi!

Nên update thường xuyên bằng cách set-up tự động theo sự hướng dẫn. Có nghĩa là khi nào nhà sản xuất có thông tin mới về virus, thì máy PC của quý vị tự động update ngay ở hậu trường (behind the scenes) trong lúc quý vị đang dùng máy PC.

Không connect với bất kỳ máy khác và share hard-disk cho bất cứ ai.

Thường xuyên backup (hàng ngày hoặc hàng tuần tùy theo sử dụng) vào CDs, DVDs... và cất riêng một chỗ để lỡ ngày sau khi ta gặp mấy nàng virus còn có chỗ mà phục hồi.

2) Spam Mail?

Đây là các email thường chứa các loại quảng cáo được gửi một cách vô tội vạ và nơi nhận là một danh sách rất dài gửi từ các cá nhân hay các nhóm người và nội dung của loại thư này thường thấp. Đôi khi, nó dẫn dụ người nhẹ dạ, tìm cách đọc số thể tín dụng và các tin tức cá nhân của họ.

Các thư gửi từ Woodard, whonysald, tara crisp, serena555, Serena Mcclain, Santiago Ritchie, Pearl Mayers, nplroeom rrsi, Nina Garcia, cũng như những emails từ Anh Quốc, Phi Châu dụ khị là trúng số, hoặc cho gia tài của người chết... là các “Spam mail”

Khi hình ảnh sản phẩm nào đó cứ đập vào mắt mình mãi thì đến lúc cần mua một thứ nào đó tương tự hay cùng loại thì chính hình ảnh quảng cáo của cái spam mail sẽ hiện đến trong óc chúng ta trước tiên. Hoặc giả đôi khi "lỡ tay" hay chỉ vì tò mò mà chúng ta bấm vào (click) vào cái link và thế là "lưới nhện đã giăng sẵn chỉ chờ con mồi ...."

Spam mail không làm hại đến computer, chỉ làm chúng ta bực mình khó chịu khi thấy chúng tự động pop-up lên.

Một chữ gần nghiã với Spam mail là Junk mail. Junk mail chỉ khác spam mail ở chỗ là nội dung của nó không phải là quảng cáo (nhằm làm cho Internet bi tắt nghẽn chẳng hạn???) và được gửi đi từ địa chỉ một hộp thư.

Cách chế ngự:

Một số các nơi cung cấp email cũng đã có sẵn filter để loại bỏ các spam mail này trước khi tới tay người nhận một cách chủ động, nhưng dĩ nhiên là không hoàn toàn 100%.

Một số khác (như là MS Outlook version 2000 hay mới hơn) cho phép chúng ta cài lại một số dấu hiệu và loại bỏ spam mail qua các thực đơn sẵn có.

Nhu liệu chống spam mà một số nhà sản xuất đã tung ra thị trường để giúp người tiêu dùng. Tuy nhiên, không phải nhu liệu nào được bán ra thị trường cũng hoạt động hữu hiệu! Hiện nay, nhu liệu chống spam tốt nhất đó là công ty Norton, McAfee AntiSpam, và Qurb 2.0.

Xử dụng WEB mail. Thay vì dùng các mail box miễn phí thì hãy dùng các dịch vụ cung cấp email qua Internet. Bằng cách này thì người chủ mail tưởng chừng đã "bán cái" trách nhiệm lọc spam mail cho các dịch vụ cung cấp. Nhưng khổ nổi là không chắc dịch vụ nào cũng chịu "Quảy gánh" lo dùm cho quý vị. Trong các dịch vụ kiểu này thì có Mailblocks Extended Servivce khá hữu hiệu (nhưng thủ tục "đầu tiên" thì không ít; giá 9.95USD trong 1 năm cho hộp thư 15MB và 24.95USD trong 1 năm cho hộp thư 100MB).

Một số chính phủ do áp lực của người dân, trong đó tiên phong là Hoa Kỳ đã có biện pháp mạnh mẽ hơn để bảo vệ người tiêu dùng bằng cách ra các đạo luật phạt khắc khe các cơ sở hay cá nhân dùng spam mail. Tuy nhiên, nhược điểm của phương án này là: 3/4 các spam mail lại không được gửi ra trong nước mà là chúng đến từ những nơi chưa có lệnh cấm!!!!

Hiện tại đang có nhiều nỗ lực để phát triển những tiêu chuẩn về mail mới ngõ hầu chấm dứt tình trạng này.

3) Spyware & Adware (chương trình gián điệp?) là gì?

Đây là loại nhu liệu chuyên thu thập các thông tin từ các máy chủ (thông thường vì mục đích thương mại) qua mạng Internet mà không có nhận thức của chủ máy. Một cách điển hình, Spyware được cài đặt một cách bí mật như là một bộ phận kèm theo của các chương trình freeware và shareware mà người ta có thể đưa về từ Internet. Một khi nhu liệu đã cài đặt, spyware điều phối các hoạt động của máy chủ trên Internet và lặng lẽ chuyển các dữ liệu thông tin đến một máy khác (của những tay hacker dĩ nhiên!) Spyware cũng thu thập tin tức về địa chỉ e-

mail và ngay cả mật khẩu cũng như là số thẻ tín dụng!!

Tác hại:

Ngoài các vấn đề nghiêm trọng về đạo đức và tự do cá nhân bị xâm phạm, Spyware còn đánh cắp từ máy chủ các tài nguyên của memory resource rồi nó gửi thông tin trở về chủ của các spyware qua Internet vàcó thể dẫn tới hư máy..

Bởi vì là một chương trình độc lập nên Spyware có khả năng điều khiển các keystroke, đọc các tin tức trong hard-disk, kiểm soát các ứng dụng khác như là chương trình chat hay chương trình soạn thảo văn bản, cài đặt các spyware mới, đọc cookies thay đổi trang nhà trên WEB browser, cung cấp liên tục các thông tin trở về chủ của Spyware và có thể dùng nó cho quảng cáo hoặc tiếp thị hay bán tin tức cho các chỗ khác.

Dấu hiệu máy bị spyware:

Bất kỳ một trong các dấu hiệu sau đây xảy ra cũng có thể là máy của quý vị đã bị ... Spyware!!!

Nhận email với giấy biên nhận trả tiền điện thoại có thêm số trả phụ trội mà quý vị chẳng bao giờ gọi tới số đó, như: bắt đầu bằng 900.

Khi gõ tìm một địa chỉ trên Internet Explorer và nhấn Enter để bắt tìm kiếm thì trang "search" thường dùng bị thay bởi 1 trang search lạ.

Các program chống Spyware không hoạt động được. Nó có thể báo lỗi mất những file cần thiết, ngay cả sau khi cài đặt trở lại thì cái chương trình chống Spyware cũng không hoạt động được.

Thấy những tên địa chỉ lạ trong danh sách Favorites mặc dù quý vị chưa hề đặt nó vào trong mục này.

Máy tự nhiên chạy chậm hơn thường nhật. Nếu là Windows 2K hay XP hãy thử chạy Task Manager và nhấn processes thì thấy những process không quen biết dùng gần như 100% CPU.

Một cái "seach toolbar" (băng tìm kiếm) hay "browser toolbar" xuất hiện mặc dù quý vị không hề cài đặt nó và không thể xoá chúng hay là chúng xuất hiện trở lại sau khi xoá.

Quý vị nhận 1 pop-up quảng cáo khi cái "browser" chưa hề được chạy và ngay cả khi máy chưa connect với Internet hay là quý vị được các quảng cáo có đề tên quý vị trong đó.

Trang nhà bị đổi một cách kỳ lạ. Quý vị đổi nó lại nhưng nó lại bị sửa ...

Ở thời điểm mà quý vị không hề làm gì với internet mà vẫn thấy đèn gửi/nhận chớp sáng trên dial-up hay board band modem giống như là khi đang download phần nhu liệu nào về máy. Hay là các hiện tượng network/modem nhấp nháy nhanh khi quý vị không hề vào internet.

Dấu hiệu cuối cùng, mọi thứ hình như trở về bình thường. Những Spyware mạnh thường không để dấu tích gì cả. Nhưng hãy kiểm lại máy của mình ngay cả trong trường hợp này.

Phòng ngừa:

Trong các bản giao kèo về bản quyền xử dụng (License Agreement) của các công ty cho download đôi khi có nói rõ rằng họ sẽ cài spyware chung với nhu liệu. Những cái giao kèo này thường ít được chúng ta đọc hoàn tất một cách kỹ lưỡng và cũng bởi vì các lưu ý về cài đặt spyware thường nằm trong những đoạn khó thấy (chữ nhỏ xíu không đọc chết ráng chịu!). Do đó trước khi download về máy bất kỳ một nhu liệu nào hãy đọc kỹ các điều luật này.

Hãy dùng nhu liệu chống Spyware. Kiểm nghiệm (scan) thường xuyên để loại bỏ spyware. Restart lại máy và chạy kiểm lại lần nữa sau mỗi lần lại được Spyware mới để chống sự tái nhiễm. Nên làm vài lần trong tuần.

Phải có chương trình chống virus và tường lửa (firewall) cho máy (chương trình tường lửa miễn phí ở www.sygate.com, www.zonelabs.com ...)

Coi chừng các dịch vụ peer-to-peer chia sẽ chung các tin tức (peer-to-peer files sharing service). Hầu hết các ứng dụng thông dụng sẽ có spyware trong các thủ tục cài đặt. Tránh download các nhu liệu tầm bậy mà chúng ta không biết ngoại trừ chúng được cung cấp từ các nhà sản xuất lớn hay các trang website "tốt".

Coi chừng các cookies; các dữ liệu thu thập bởi các cookies có thể trùng lặp với các thông tin ở 1 nơi nào đó để cung cấp những thông tin của quý vị một cách đáng ngạc nhiên. Quý vị có thể download chương trình Cookie Cop 2 từ trang www.pcmag.com/utilities để kiểm soát các cookie.

Hãy sửa mức an toàn của browser cao lên ít nhất là medium và không cho phép cài đặt tất cả các "ActiveX control" mà quý vị chưa yêu cầu.

Spyware có thể đến từ các HTML e-mail. Hãy thẳng tay delete những email mà quý không biết rõ xuất xứ và không hề có liên lạc, hoặc email có địa chỉ quen thuộc nhưng chủ đề rất lạ (do tụi hackers gửi đi). Nếu dùng Outlook 2003, dùng Tools -> Options -> Security tab -> chọn "change Automatic Download Settings". Kiểm chắc rằng quý vị đã chọn "Don't download pictures or other content automatically in HTML email".

Hiện nay có một số nhu liệu miễn phí chống mấy chú em này, tuy không 100% nhưng cũng được 80 đến 90%. Trong đó là: Ad Aware, Spybot, Spyware Doctor, Windows Defender...

Download nhu liệu chống Spyware & Adware tại đây

Revision #1
Created 12 June 2023 11:02:19 by Quản trị
Updated 12 June 2023 11:02:43 by Quản trị