MOET CICT
BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRUNG TÂM TIN HỌC

MỘT SỐ VẤN ĐỀ CÓ LIÊN QUAN ĐẾN VIRUS MÁY TÍNH

(Tài liệu được sưu tầm trên Internet)

CÁC CÂU HỎI CHUNG VỀ VIRUS MÁY TÍNH

Virus máy tính là gì ?

Virus máy tính là một chương trình phần mềm, xin nhấn mạnh với các bạn nó là một chương trình, và chương trình này được thiết kế để có thể lây lan ra các file chương trình hoặc các khu vực hệ thống của đĩa cứng hay đĩa mềm, đặc điểm đặc trưng của chúng là khả năng tự nhân bản.Virus luôn luôn có thể tự mình làm mọi việc mà không cần có sự cho phép của người sử dụng, nhưng tất nhiên là lần đầu tiên phải có một thao tác nào đó của người sử dụng kích hoạt nó lên (do không biết đó là virus).

Virus máy tính lây lan như thế nào ?

Khi bạn chạy một chương trình đã bị lây bởi một virus, thì chương trình virus sẽ được kích hoạt và cố gắng để lây vào các chương trình khác, trên máy tính của bạn hay có thể là lan ra cả mạng Internet nếu như máy tính của bạn có kết nối Internet. Quá trình nhân bản cứ tiếp tục như vậy theo cấp số nhân. Quá trình lây lan của virus diễn ra một cách "âm thầm", người sử dụng sẽ không nhận ra điều đó vì sau khi thực hiện xong công việc lây lan, chương trình bị lây nhiễm vẫn chạy bình thường và như thế thì bạn khó có thể nhận biết được sự tồn tại của chúng khi chúng chưa phá hoại. Chúng xứng đáng được một huân chương cho điệp viên bí mật hạng ưu.

Nếu máy tính bị lây nhiễm virus boot, thì virus sẽ cố tự ghi mình vào phần dùng để khởi động máy trên đĩa cứng hay đĩa mềm. Và nếu máy tính khác sử dụng những đĩa này để khởi động, thì virus lại tiếp tục có chỗ dung thân, chúng sẽ lại tiếp tục nhảy vào khu vực hệ thống yêu thích của chúng trên máy tính nạn nhân này.

Loại file nào có thể phát tán Virus ?

Ngày nay có thể nói virus có thể lây nhiễm bất cứ loại file nào mà trong đó có chứa những đoạn mã chương trình mà máy tính có thể "chạy" được, không chỉ những file mà vẫn thường được gọi là file chương trình như .COM, .EXE, .BAT.... Ví dụ, một số virus có thể lây nhiễm các mã thực thi trong boot sector của đĩa mềm hay trong một số khu vực hệ thống của đĩa cứng. Và một số loại virus khác, ví dụ như virus macro, có thể lây nhiễm vào chương trình soạn thảo sử dụng macro của bộ Microsoft Office .DOC, .DOT, .XLS...

Virus sẽ làm gì với máy tính?

Sau khi đã viết ra một virus máy tính thì phần gây tác hại có lẽ là phần mà đa số những kẻ viết virus đều rất lưu tâm. Chúng có thể cho virus này tàn phá nặng nề ổ đĩa, hệ thống nếu chúng là người ác ý, hay đơn giản chỉ là một câu đùa vui hay nghịch ngợm đôi chút với màn hình nếu đó là một kẻ vui tính. Tuy nhiên cũng có một số virus máy tính không phá hoại gì mà chỉ nhân bản lên. Nhưng như thế đôi khi cũng thành phá hoại, vì trong quá trình lây lan chúng có thể vô tình phá hoại dữ liệu của máy tính.

Chúng ta có phải sợ virus không?

Virus máy tính không phải là quỷ dữ, chúng chỉ là các chương trình có thể tự nhân bản trong máy tính cũng như qua mạng. Các chương trình diệt được thiết kế để diệt chúng. Nếu được cập nhật thường xuyên thì các chương trình diệt có thể diệt được hầu hết các loại virus. Phải cập nhật thường xuyên vì mỗi loại virus mới xuất hiện sẽ phải cần những phương pháp diệt khác nhau, không thể có chương trình diệt virus nào mà có thể diệt được tất cả các laọi virus, cũng như đối với virus sinh học vậy, không có loại kháng sinh nào tiêu diệt được hết bọn chúng.

Virus có thể ẩn mình trong CMOS của máy tính được không?

Câu trả lời là không. Dữ liệu trong CMOS không phải là các chương trình thực thi được. CMOS chỉ đơn thuần chứa dữ liệu hệ thống, đó là cấu hình của máy tính, chúng được lưu trong một con chip bên trong máy tính. Một virus có thể thay đổi hay xoá dữ liệu trong CMOS, chứ không thể lây lan hay giấu mình vào đó được.

Có virus BIOS không ?

Theo lý thuyết, có thể có virus ẩn mình trong BIOS và được thực hiện từ BIOS vì ở đó có mã chương trình thực thi được. Công nghệ hiện thời cho phép chương trình viết mã lệnh vào trong BIOS. BIOS là nơi lưu trữ phần đầu của chương trình được thực hiện khi PC khởi động. Tuy nhiên gần như chưa xuất hiện loại virus như thế.

Đĩa khởi động sạch là gì, và làm thế nào có thể tạo một đĩa khởi động sạch ?

Là một đĩa chứa các file cần thiết để khởi động một hệ điều hành. Nếu ở hệ điều hành DOS, để tạo đĩa khởi động thì phải đảm bảo là máy tính bạn sử dụng để tạo cái đĩa đó không bị nhiễm virus và gõ lệnh: Format /s a:

Nếu là Windows95/98 thì có thể tạo đĩa khởi động bằng cách chọn "Add/Remove Program" trong Control Panel, tiếp đến chọn Startup Disk và nhấn vào "Create Disk". Sau khi tạo đĩa phải đảm bảo rằng chúng được đặt chế độ "Write protected" để từ đó chúng không bị nhiễm virus.

Một số files bị nhiễm CIH mà không thể diệt được trong Windows ?

Đúng là một số phần mềm của nước ngoài hay báo như vậy, nhưng điều này không xảy ra với BKAV.

Tại sao một số virus có thể nhận diện được nhưng không thể diệt được với một số phần mềm chống virus

Trong quá trình lây nhiễm, một số file chương trình có thể bị virus làm hỏng và không thể khôi phục được nữa. Trong trường hợp đó các phần mềm diệt virus chỉ có thể báo là có virus, nhưng không thể diệt được.

Tình huống thứ 2 là: một số phần mềm diệt virus có tính năng "phán đoán" virus mà hay được gọi là tính năng "thông minh", có nghĩa là nó sẽ phân tích và đưa ra nghi ngờ sự xuất hiện của virus, chứ không khẳng định được chính xác là có virus hay không. Như vậy sẽ có 2 khả năng, một là phần mềm phán đoán nhầm, hai là đoán đúng, nhưng trong cả 2 khả năng thì cũng đều không thể diệt được virus vì việc diệt virus không hề đơn giản, nhất là khi chưa xác định chính xác virus đó là gì.

Tình huống thứ 3: File bị nhiễm virus là file hệ thống, tức là nó đang được hệ thống, mà ở đây là hệ điều hành sử dụng. Vì vậy mà phần mềm diệt virus không thể nào can thiệp vào những file đó được (đây là quy định của hệ điều hành). Do không có quyền can thiệp vào những file đó, phần mềm sẽ không thể diệt virus trên file được. Tuy nhiên điều đó sẽ không xảy ra đối với Bkav, do trong Bkav có một số công nghệ đặc biệt xử lý tình huống này.

Virus hay chỉ là những sự cố máy tính ?

Như các bạn đã biết, hiện nay có rất nhiều loại virus máy tính xuất hiện và các hình thức phá hoại của chúng cũng rất đa dạng và ngày càng nguy hiểm. Vì thế, việc nghi ngờ và đề phòng virus tấn công máy tính của chúng ta, đã dường như đã trở thành một phản xạ tự nhiên mỗi khi gặp một vấn đề lạ khi sử dụng máy tính.

Tuy nhiên không phải tất cả những sự cố xảy ra trên máy tính của bạn đều do virus gây ra và để xử lý chúng ta sẽ phải mất rất nhiều thời gian mà không đạt được kết quả gì nếu chúng ta cho rằng đó là do virus. Hay nói cách khác, đôi khi chúng ta cũng đổ oan chi virus. Trong thực tế 7 năm qua trong việc trả lời cho người sử dụng các thắc mắc về virus máy tính, chúng tôi thấy phải tới trên 50% các thắc mắc về chục trặc của máy tính không phải do virus gây ra.

Chúng ta có thể sẽ không phải mất nhiều thời gian như thế nữa nếu biết được một số sự cố thường gặp mà nguyên nhân có thể không phải là do virus.
Hàng ngày chúng tôi nhận được rất nhiều email và điện thoại trong đó có nhiều khách hàng hỏi tư vấn về các vấn đề thường gặp như :

+ Máy tính của bạn bị treo khi bạn đang làm việc
+ Chương trình soạn thảo Word của bạn xuất hiện những ký tự lạ
+ Chương trình của bạn tự nhiên không chạy
+ Máy tính của bạn không khởi động được và có thông báo lỗi
+ Máy tính của bạn đưa ra thông báo có Virus boot khi bạn cài Windows hay một chương trình hệ thống nào đó
+ Bạn không thể cài được Windows vì cứ chạy cài đặt là máy bị treo...

Và điều tất nhiên là mọi người nghi ngay can phạm là virus! Sự thực không phải thế, những thông tin sau sẽ giúp bạn một phần nào:

Máy tính của bạn bị treo khi bạn đang làm việc?

Hiện tượng máy tính bị treo khi bạn đang làm việc hoặc khi khởi động lại chỉ được 10 đến 15 phút nó lại treo. Hiện tượng này thường là do Chip máy tính của bạn bị nóng, nguyên nhân có thể quạt Chip của bạn bị hỏng hoặc là chạy chậm, trong trường hợp này bạn có thể kiểm tra nguồn cho quạt hoặc tra dầu cho quạt, nếu trường hợp quạt bị hỏng bạn nên thay quạt cho Chip. Ngoài ra cũng có thể do RAM hay Mainboard có vấn đề. Sau khi kiểm tra hết các vấn đề đó bạn hãy đặt nghi vấn cho virus.

Chương trình soạn thảo Word của bạn xuất hiện những ký tự lạ?

Chúng tôi đã nhận được rất nhiều thư và điện thoại các bạn hỏi về vấn đề này, và gần như tất cả đều do một nguyên nhân là trên thanh công cụ của Microsoft Word có một phím gọi là phím Show/Hide (nó có biểu tượng là "¶") phím này có tác dụng làm hiện hoặc ẩn các kí tự đặc biệt mà Word dùng để chỉ định các định dạng của nó, các dấu hiệu paragraph hoặc các kí tự ẩn, những thứ này thường chỉ phục vụ cho bản thân Microsoft Word biết về định dạng của văn bản, còn người sử dụng thì không cần phải biết đến. Tuy nhiên, đôi khi người sử dụng cũng có nhu cầu hiện những thông tin này lên, và đó là nguyên nhân của một loạt các ký tự lạ xuất hiện khắp màn hình. Nếu gặp phải hiện tượng này bạn chỉ cần tìm trên thanh công cụ phím bấm có biểu tượng "¶" và bấm chuột vào phím đó, các ký tự lạ sẽ mất đi.

Chương trình của bạn tự nhiên không chạy?

Có thể vào một ngày nào đó, khi bạn bật máy tính của mình lên và click vào biểu tượng của chương trình mà bạn vẫn dùng hàng ngày và thật là kỳ lạ, thay vào giao diện của chương trình quen thuộc là một thông báo lỗi rất khó hiểu của Windows sau đó nó không chịu làm gì nữa. Nếu bị rơi vào trường hợp này thì bạn hãy chịu khó đọc qua thông báo lỗi xuất hiện. Các thông báo này thường là: Không tìm thấy file chương trình, không tìm thấy file dữ liệu nào đó, không tìm thấy file dll ... Đối với những thông báo như vậy, bạn chỉ cần ghi nhớ tên file mà thông báo chỉ ra, sau đó bạn sử dụng công cụ Search của Windows tìm file đó trên máy tính của bạn, nếu thấy bạn hãy copy file đó vào thư mục của chương trình, sau đó bạn cho chạy lại chương trình nếu không được bạn hãy thử cài lại chương trình của bạn.
Đôi khi có một số chương trình có yêu cầu bản quyền mà phiên bản bạn dùng lại là bản dùng thử, và khi bạn chạy chương trình vào thời điểm hết thời gian dùng thử thì chương trình thường đưa ra thông báo lỗi. Trong trường hợp này bạn phải liên hệ với nhà cung cấp để mua bản chính thức.

Máy tính của bạn không khởi động được và có thông báo lỗi?

Máy tính của bạn bỗng nhiên khi khởi động lại đưa ra thông báo "Invalid system disk..." hoặc "System disk error..." thì có lẽ trong ổ đĩa mềm của bạn đang chứa một đĩa mềm nào đó không có file hệ thống, bạn hãy lấy đĩa mềm đó ra và khởi động lại máy, mọi việc sẽ ổn.

Máy tính của bạn đưa ra thông báo có Virus boot khi bạn cài Windows hay một chương trình hệ thống nào đó?

Trên một số MainBoard, nhà sản xuất thường tạo thêm một chức năng trong CMOS đó là "tự động bảo vệ trước virus" nhưng thực tế thì chức năng này luôn đưa ra cảnh báo khi một chương trình nào đó (Kể cả nó không phải là virus) ghi thông tin lên boot sector của đĩa cứng, và không cho phép chương trình làm việc đó nữa. Để giải quyết vấn đề này bạn hãy vào CMOS và "Disable" chức năng này đi, chương trình của bạn sẽ lại làm việc bình thường.

Bạn không thể cài được Windows vì cứ chạy cài đặt là máy bị treo?

Lỗi này có thể là đĩa cứng của bạn bị trục trặc về phần cứng và cũng có thể RAM của bạn bị lỗi. Để xử lý tình huống này bạn phải kiểm tra lại phần cứng của máy, xem có thiết bị nào bị lỏng hay không, nếu không được có lẽ bạn phải gọi cho người bảo hành.