Virus Máy Tính – Phòng và Chống

1. Virus máy tính là gì?

a. Định nghĩa:

Virus máy tính là những đoạn mã chương trình được viết ra để thực hiện tối thiểu hai việc:

- Tự xen vào hoạt động hiện hành của máy tính để thực hiện những công việc theo chủ ý của người lập trình, sau khi kết thúc thực thi mã virus thì điều khiển được trả lại cho chương trình đang thực thi mà máy không bị treo, trừ trường hợp virus cố ý làm treo máy.
- Tự sao chép chính nó, tức tự nhân bản, vào các tập tin hay các vùng xác định ở các thiết bị lưu trữ như đĩa cứng, đĩa mềm, các thiết bị nhớ (USB), …

Chương trình: Được tạo thành từ một dãy gồm rất nhiều các dòng lệnh dưới dạng mã máy (machine code – dạng mã mà máy tính có thể hiểu và thực thi) liên tiếp nhau được đóng gói lại chờ thực hiện (ví dụ dưới dạng file có đuôi .exe trong Windows). Khi chương trình được chạy, các mã lệnh của chương trình được copy vào RAM, sau đó CPU sẽ thực hiện lần lượt từng lệnh được copy vào RAM bắt đầu từ lệnh đầu tiên.

Chương trình máy tính, là một chuỗi các lệnh; nó khác với phần mềm máy tính. Phần mềm máy tính là tập hợp của một hoặc nhiều chương trình máy tính và các dữ liệu liên quan.

b. Cách thức hoạt động, lây lan:

Virus hoạt động và lây lan trong máy tính thông qua việc tìm cách thâm nhập vào các chương trình đang thực thi trên máy tính. Virus ngắn có thể gắn thêm vào tệp mã của chương trình hoặc có thể lưu trữ phần thân ở dạng file riêng và ẩn dấu đâu đó trong đĩa hoặc trên mạng, và nội dung file này có thể là dạng macro hoặc html. Một số virus thì xuất hiện ở dạng chương trình tự lập, thực chất là phần mềm phá hoại, và thực hiện đánh lừa bằng cách hiện ra là một biểu tượng (icon) hay đường link để người thiếu cảnh giác click vào đó.

Có rất nhiều con đường mà virus có thể lợi dụng để xâm nhập vào máy tính. Virus có thể lây qua mạng nội bộ (mạng LAN), qua email, qua các đường link hay file tải về từ Internet hay từ các ổ đĩa USB chứa virus. Tinh vi hơn, chúng có thể lợi dụng các lỗ hổng phần mềm, kể cả hệ điều hành để xâm nhập, lây nhiễm lên máy tính thông qua mạng Internet.

c. Quá trình phát triển của virus máy tính:

Virus máy tính có một quá trình phát triển khá dài kể từ lần đầu tiên xuất hiện vào năm 1981. Khi công nghệ phần mềm cũng như phần cứng phát triển thì virus máy tính cũng phát triển theo. Hệ điều hành thay đổi thì virus máy tính cũng phải thay đổi để có thể ăn bám, ký sinh trên hệ điều hành mới. Chính vì vậy, các khái niệm virus máy tính cũng luôn được hình thành và mở rộng dần theo thời gian.

Ban đầu, virus máy tính được định nghĩa là một chương trình phần mềm có khả năng tự sao chép chính nó từ đối tượng lây nhiễm này sang đối tượng khác (đối tượng có thể là các ổ đĩa mềm, đĩa cứng, các file chương trình, văn bản ...). Virus được viết ra cho những mục đích phá hoại, thử nghiệm hay đơn giản chỉ là một thú đùa vui (nhiều khi ác ý), nhưng nói chung, nó là chương trình máy tính được viết ra để thực hiện những dòng lệnh trái với mong muốn của người sử dụng máy tính.

Sau này khi công nghệ phát triển kéo theo sự ra đời của nhiều loại phần mềm nguy hại khác, các phần mềm đó vẫn được gọi chung là virus máy tính. Bởi tuy không có cơ chế tự động lây nhiễm như virus nhưng chúng vẫn có một đặc điểm chung, đó là được dùng trong những mục đích không tốt.

2. Các loại malware:

Một số loại malware:

* Worm: là các chương trình cũng có khả năng tự nhân bản tự tìm cách lan truyền qua hệ thống mạng (thường là qua hệ thống thư điện tử). Sâu máy tính thường được thiết kế để khai thác khả năng truyền thông tin trên những máy tính có các đặc điểm chung - cùng hệ điều hành hoặc cùng chạy một phần mềm mạng - và được nối mạng với nhau. Ngoài gây tác hại cho máy bị nhiễm, nhiệm vụ chính của worm là phá các mạng (network) thông tin chia sẻ, làm giảm khả năng hoạt động hay ngay cả hủy hoại các mạng này.

Ví dụ: virus Melissa là một loại macro virus xuất hiện vào năm 1999 do David L. Smith tạo ra, virus này có tốc độ lây truyền nhanh qua một file được đính kèm trong email. Khi người nhận mở file, virus sẽ tự động được gửi tiếp đến 50 người đầu tiên trong danh sách sổ địa chỉ Microsoft Outlook của người dùng. Melissa virus không làm hư hại dữ liệu hay các tài nguyên trong máy tính nhưng nó có thể ảnh hưởng và làm vô hiệu hóa các hệ thống máy chủ khi số lượng email được gửi tự động tăng theo cấp số nhân đến một con số quá lớn.

* Ransomware: là một loại malware (phần mềm mã độc) ngăn chặn hoặc giới hạn người dùng sử dụng thiết bị, hệ thống hoặc dữ liệu của mình. Khi ransomware lây nhiễm vào máy tính, nó có thể khóa thiết bị của bạn lại hoặc mã hóa một phần hay toàn bộ dữ liệu trong ổ cứng. Nó sẽ để lại lời nhắn để buộc nạn nhân phải trả tiền để có quyền sử dụng tiếp hệ thống của họ.

Ransomware có thể bị download xuống máy người dùng bằng nhiều cách khác nhau như: lừa người dùng vào một website giả mạo hoặc website đã bị chèn mã độc, đính kèm trong email gửi đến người dùng. Bên cạnh đó, ransomware còn tận dụng các lỗ hổng bảo mật của hệ điều hành hoặc các phần mềm để lây nhiễm và chạy.

Ví dụ: Những trường hợp đầu tiên bị dính ransomware được ghi nhận là tại Nga vào năm **2005 - 2006**. Ransoware mang số hiệu TROJ_CRYZIP.A đã nén các tập tin quan trọng của người dùng lại thành một file zip rồi xóa đi các tập tin gốc. Để mở file zip này thì cần có password. TROJ_CRYZIP.A còn tạo một file văn bản để làm "thư tống tiền", trong đó nói rằng người dùng muốn có password để mở file zip thì phải trả 300$.

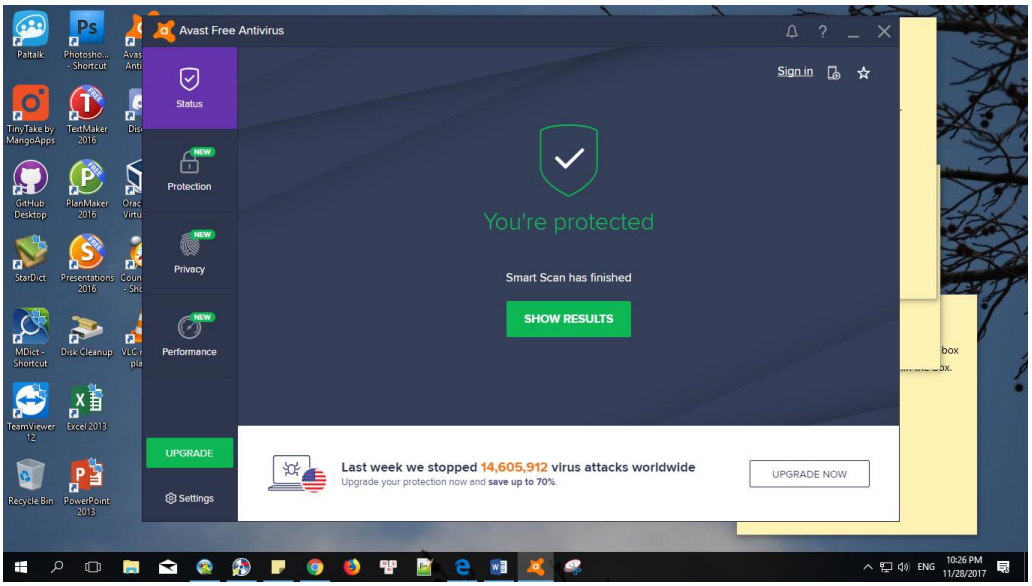
*Spyware (phần mềm gián điệp): là loại phần mềm chuyên thu thập các thông tin từ các máy tính qua mạng Internet mà không có sự nhận biết và cho phép của người dùng. Spyware thường được cài đặt một cách bí mật như là một bộ phận kèm theo của các phần mềm miễn phí và phần mềm chia sẻ mà ta có thể tải về từ Internet. Một khi 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. Phần mềm gián điệp cũng thu thập tin tức về địa chỉ thư điện tử và ngay cả mật khẩu cũng như số thẻ tín dụng…

Ví dụ: WildTangent, là spyware được cài đặt thông qua American Online Instant Messenger (AIM). Một khi được cài đặt, nó sẽ lấy các thông tin về tên họ, số điện thoại, địa chỉ thư điện tử cũng như là tốc độ của CPU, các tham số của video card và DirectX gửi về máy tính điều khiển. Sau đó các thông tin này có thể bị chia sẻ cho các nơi khác chiếm dụng nhằm mục đích thương mại hoặc quảng cáo.

3. Cách phòng chống malware:

a. Kiểm tra máy tính có bị lây nhiễm malware:

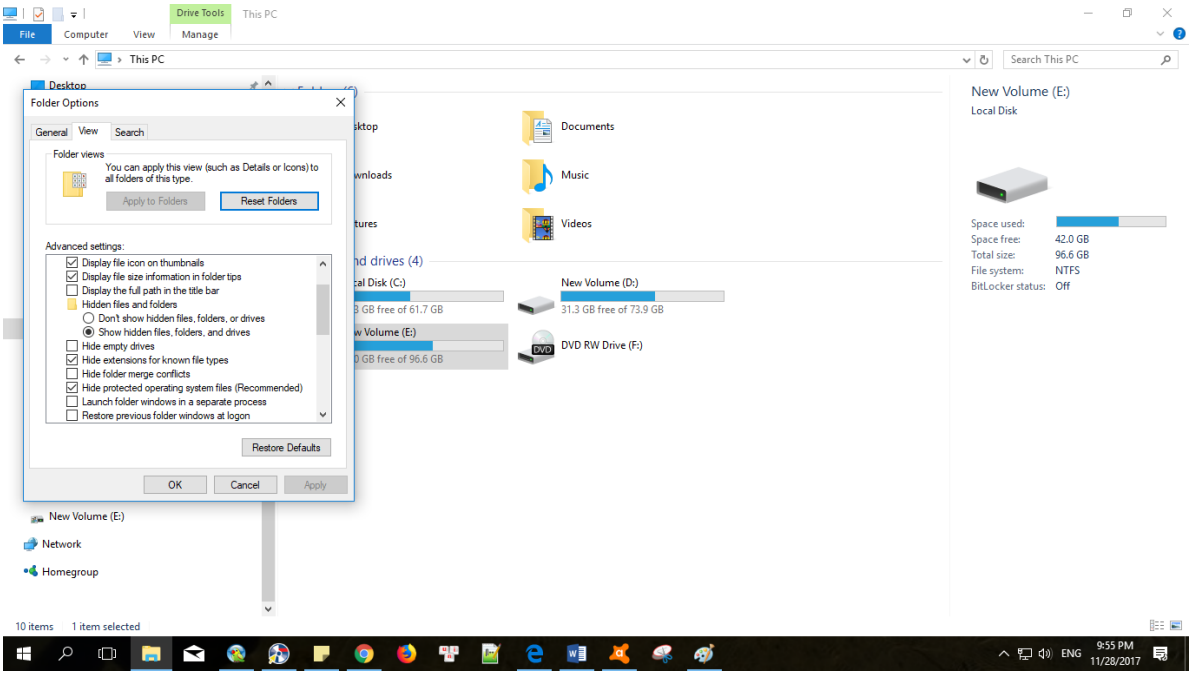
-B1: Chạy phần mềm diệt virus máy tính (Avast).



-B2: Kiểm tra có file lạ ẩn trong ổ dữ liệu.

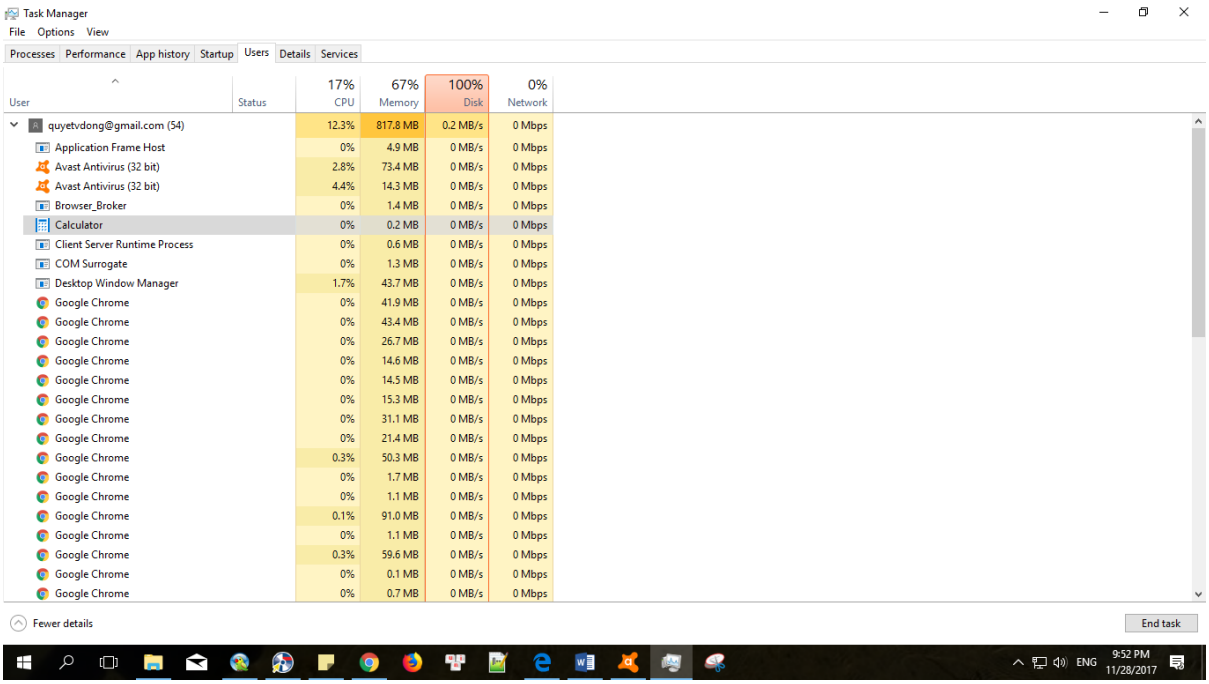
Vào File Explorer -> chọn View -> chọn Folder Option -> chọn View -> tích chọn “Show hidden files, folders and drives”. Sau đó nhấn Apply -> OK.

Tiếp tục vào File Explorer -> chọn View -> chọn Folder Option -> chọn View -> kiểm tra nếu dòng “Show hidden files, folders and drives” vẫn được tích thì có thể an tâm.



-B3: Kiểm tra các chương trình đang thực thi trong Task Manager.

Vào Task Manager -> User để kiểm tra các trình thực thi trong máy tính.



-B4: Theo dõi máy tính không bị chậm đột ngột, không đột nhiên bị treo hay có hiện tượng gì bất thường.

Kết luận máy tính không bị nhiễm Malware.

b. Các phương pháp an toàn chống lây nhiễm malware:

- Không mở email lạ có địa chỉ người gửi không rõ nguồn gốc

- Tắt chức năng tự động hiển thị ảnh trong email

- Không download các file đáng nghi hoặc không rõ ràng được đính kèm trong email

- Không vào các trang web lạ, không đáng tin

- Không download dữ liệu hoặc chương trình không rõ nguồn gốc hoặc chưa được xác minh an toàn

- Kiểm tra các đường link trước khi click, không click vào các đường link không rõ ràng lan truyền trên internet (qua email, chat, mạng xã hội,…). Thay vì click link có thể đánh trực tiếp địa chỉ trang web.

- Theo dõi hoạt động của máy tính

- Chạy chương trình quét virus định kỳ (1 tuần 1 lần hoặc vài ngày một lần tùy theo nhu cầu sử dụng máy tính)

- Bật Firewall để bảo vệ máy tính

- Sử dụng các chương trình và phần mềm an toàn, có uy tín

- Thường xuyên cập nhật hệ điều hành và các chương trình trong máy tính