Computer Virus

By

Nguyễn Thành Doanh
FFSE1702062

CÁC KHÁI NIỆM LIÊN QUAN

Trước hết ta cần tìm hiểu cách máy tính và một chương trình máy tình hoạt động ra sao

- **Ngôn ngữ máy** (machine language hay machine code) là một tập các chỉ thị được CPU của máy tính trực tiếp thực thi. Mỗi chỉ thị thực hiện một chức năng xác định, ví dụ như tải dữ liệu, nhảy hay tính toán số nguyên trên một đơn vị dữ liệu của thanh ghi CPU hay bộ nhớ.
- **Chỉ thị máy tính** (instruction) là đơn vị nhỏ nhất dùng để điều khiển máy tính, cụ thể hơn là ra lệnh cho CPU thực hiện một thao tác căn bản.
- **Chương trình máy tính** thực chất chỉ là một chuỗi những chỉ thị viết bằng mã máy được thực thi bởi CPU. Nói 1 cách đơn giản, **Chương trình máy tính** là một dạng hoạt động thủ công nhưng được chuyển đổi sang dạng yêu cầu thành một thứ mà máy tính có thể thi hành được.
- **Phần mềm máy tính** (Computer Software) hay gọi tắt là Phần mềm (Software) là một tập hợp những câu lệnh hoặc chỉ thị (Instruction) được viết bằng một hoặc nhiều ngôn ngữ lập trình theo một trật tự xác định, và các dữ liệu hay tài liệu liên quan nhằm tự động thực hiện một số nhiệm vụ hay chức năng hoặc giải quyết một vấn đề cụ thể nào đó
- **Virus** máy tính 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 file chương trình, văn bản, máy tính...). Virus có nhiều cách lây lan và tất nhiên cũng có nhiều cách phá hoại, tóm lại đó là một đoạn chương trình và đoạn chương trình đó thường dùng để phục vụ những mục đích không tốt

CÁCH THỨC HOẠT ĐỘNG VÀ LÂY LAN CỦA VIRUS

Cách thức hoạt động

- Các máy tính hoạt động bằng các chỉ thị (hay lệnh, instruction) ở dạng mã máy theo trình tự hợp lý để thực thi một công việc (task) nào đó. Mã máy là dãy số nhị phân và việc lập trình (hay thảo chương) trực tiếp mã máy rất nhức đầu, nên giới điện toán thiết kế ra các ngôn ngữ lập trình (như C, C++, Java,...) để người lập trình ứng dụng thảo chương bằng những ký hiệu và tên gọi dễ nhớ, sau đó dịch sang mã máy để máy thi hành. Nếu lập trình không hợp lý thì máy bị treo, không làm được gì.
- Kỹ thuật lập trình dẫn đến *những công việc xác định được lặp lại nhiều lần* thường được tổ chức thành modul riêng gọi là "trình con", trong ngôn ngữ lập trình gọi là *routine* hay *subroutine*, và khi cần thực hiện công việc vốn ấn

định cho routine đó thì trình đang chạy thực hiện lệnh gọi (call) đến routine đó để thực thi. Lệnh *call* có tham số là địa chỉ routine trong bộ nhớ, khi thực thi lệnh call thì chuyển địa chỉ này vào *con trỏ lệnh* của CPU và trao quyền chạy cho routine đó. Cấu trúc routine có *điểm vào* (entry) là nơi bắt đầu, và *điểm ra*(exit) trả lại điều khiển cho trình gọi (caller) sau khi hoàn tất công việc.

- Virus được viết ra là dạng một *routine*, thực hiện sửa tham số địa chỉ của một số lệnh *call* trỏ đến địa chỉ của nó, và kết thúc virus thì chuyển điều khiển đến routine vốn được gọi của trình. Những gì virus làm thì gói trong dãy mã lệnh virus, trong đó có kỹ năng tự sao lây nhiễm, và tùy thuộc trình độ người viết virus.
- Sự tương tự của mã trình với mã ADN sinh học, và hoạt động của virus tin học, dẫn đến tên gọi "*virus*". Dẫu vậy sự khác nhau căn bản, là virus sinh học phát tác ngay và đồng thời trong tế bào, còn virus tin học chỉ phát tác khi *được gọi* với tư cách mã lệnh. Nếu nạp virus tin học với tư cách dữ liệu (data) vào bộ nhớ để xem (dump) thì nó không làm được gì cả. Nó cho thấy vai trò cảnh giác khi *click* vào file có virus (tức là có thể view, edit, delete,... nhưng đừng *double click*).
- Trong thiết kế các máy tính địa chỉ các routine cơ bản được bố trí như sau:
- Địa chỉ các routine của máy chứa trong BIOS thì sau khởi động được đặt trong bộ nhớ ở nơi gọi là "bảng địa chỉ Interrupt".
- Khởi động của ổ đĩa (mềm, cứng, USB,...) được đặt ở *boot sector*, còn địa chỉ file trong ổ đĩa đặt ở bảng FAT của đĩa.
- Virus lục lọi các bảng này để tìm cách thâm nhập thích hợp. Trước đây các virus thường ngắn, có thể gắn thêm vào tệp mã. Ngày nay virus 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. Các hệ điều hành đã tăng cường bảo mật những điểm dễ bị tấn công. Vì thế virus phải cố tìm các *lỗ hổng bảo mật* để xâm nhập, và việc tìm ra lỗ hổng đòi hỏi khả năng phân tích mã lệnh phức tạp hơn. 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

Các hình thức lây nhiễm của virus máy tính

Virus lây nhiễm theo cách cổ điển

- Cách cổ điển nhất của sự lây nhiễm, bành trướng của các loai virus máy tính là thông qua các thiết bị lưu trữ di động: Trước đây đĩa mềm và đĩa CD chứa chương trình thường là phương tiện bị lợi dụng nhiều nhất để phát tán. Ngày nay khi đĩa mềm rất ít được sử dụng thì phương thức lây nhiễm này chuyển qua các ổ USB, các đĩa cứng di động hoặc các thiết bị giải trí kỹ thuật số.

Virus lây nhiễm qua thư điện tử

- Khi mà thư điện tử (e-mail) được sử dụng rộng rãi trên thế giới thì virus chuyển hướng sang lây nhiễm thông qua thư điện tử thay cho các cách lây nhiễm truyền thống.
- Khi đã lây nhiễm vào máy nạn nhân, virus có thể tự tìm ra danh sách các địa chỉ thư điện tử sẵn có trong máy và nó tự động gửi đi hàng loạt (*mass mail*) cho những địa chỉ tìm thấy. Nếu các chủ nhân của các máy nhận được thư bị nhiễm virus mà không bị phát hiện, tiếp tục để lây nhiễm vào máy, virus lại tiếp tục tìm đến các địa chỉ và gửi tiếp theo. Chính vì vậy số lượng phát tán có thể tăng theo cấp số nhân khiến cho trong một thời gian ngắn hàng hàng triệu máy tính bị lây nhiễm, có thể làm tê liệt nhiều cơ quan trên toàn thế giới trong một thời gian rất ngắn.
- Khi mà các phần mềm quản lý thư điện tử kết hợp với các phần mềm diệt virus có thể khắc phục hành động tự gửi nhân bản hàng loạt để phát tán đến các địa chỉ khác trong danh bạ của máy nạn nhân thì chủ nhân phát tán virus chuyển qua hình thức tự gửi thư phát tán virus bằng nguồn địa chỉ sưu tập được trước đó.
- Phương thức lây nhiễm qua thư điển tử bao gồm:
- ***Lây nhiễm vào các file đính kèm*** theo thư điện tử (*attached mail*). Khi đó người dùng sẽ không bị nhiễm virus cho tới khi file đính kèm bị nhiễm virus được kích hoạt (do đặc điểm này các virus thường được "trá hình" bởi các tiêu đề hấp dẫn như sex, thể thao hay quảng cáo bán phần mềm với giá vô cùng rẻ)
- ***Lây nhiễm do mở một liên kết trong thư điện tử.*** Các liên kết trong thư điện tử có thể dẫn đến một trang web được cài sẵn virus, cách này thường khai thác các lỗ hổng của trình duyệt và hệ điều hành. Một cách khác, liên kết dẫn tới việc thực thi một đoạn mã, và máy tính bị có thể bị lây nhiễm virus.
- ***Lây nhiễm ngay khi mở để xem thư điện tử:*** Cách này vô cùng nguy hiểm bởi chưa cần kích hoạt các file hoặc mở các liên kết, máy tính đã có thể bị lây nhiễm virus. Cách này thường khai thác các lỗi của hệ điều hành.

Virus lây nhiễm qua mạng Internet

- Theo sự phát triển rộng rãi của Internet trên thế giới mà hiện nay các hình thức lây nhiễm virus qua Internet trở thành các phương thức chính của virus ngày nay. Có các hình thức lây nhiễm virus và phần mềm độc hại thông qua Internet như sau:
- Lây nhiễm thông qua các file tài liệu, phần mềm: Là cách lây nhiễm cổ điển, nhưng thay thế các hình thức truyền file theo cách cổ điển (đĩa mềm, đĩa USB...) bằng cách tải từ Internet, trao đổi, thông qua các phần mềm...
- Lây nhiễm khi đang truy cập các trang web được cài đặt virus (theo cách vô tình hoặc cố ý): Các trang web có thể có chứa các mã hiểm độc gây lây nhiễm

virus và phần mềm độc hại vào máy tính của người sử dụng khi truy cập vào các trang web đó.

- Lây nhiễm virus hoặc chiếm quyền điều khiển máy tính thông qua các lỗi bảo mật hệ điều hành, ứng dụng sẵn có trên hệ điều hành hoặc phần mềm của hãng thứ ba: Điều này có thể khó tin đối với một số người sử dụng, tuy nhiên tin tặc có thể lợi dụng các lỗi bảo mật của hệ điều hành, phần mềm sẵn có trên hệ điều hành (ví dụ Windows Media Player) hoặc lỗi bảo mật của các phần mềm của hãng thứ ba (ví dụ Acrobat Reader) để lây nhiễm virus hoặc chiếm quyền kiểm soát máy tính nạn nhân khi mở các file liên kết với các phần mềm này.

DẠNG TẤN CÔNG PHỔ BIẾN CỦA HACKER: MALWARE ATTACKS

Sâu máy tính(worm)

- **Sâu máy tính** là một chương trình máy tính có khả năng tự nhân bản giống như virus máy tính. Trong khi virus máy tính bám vào và trở thành một phần của mã máy tính để có thể thi hành thì sâu máy tính là một chương trình độc lập không nhất thiết phải là một phần của một chương trình máy tính khác để có thể lây nhiễm. Sâu máy tính thường được thiết kế để khai thác khả năng truyền thông tin có 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 tác hại thẳng lên máy bị nhiễm, nhiệm vụ chính của worm là phá các mạng (network) thông tin, làm giảm khả năng hoạt động hay ngay cả hủy hoại các mạng này
- Worm thường lây nhiễm qua thư điển tử như: ***Lây nhiễm vào các file đính kèm*** theo thư điện tử, ***Lây nhiễm do mở một liên kết trong thư điện tử*** hay qua các thiết bị lưu trữ di động như ổ USB
- Dẫn chứng: Storm Worm bắt đầu nổi lên và phát tán rộng rãi trên mạng Internet vào năm 2006 theo con đường email chứa tệp tin đính kèm độc hại.Nếu người dùng lỡ tay mở tệp tin đính kèm hoặc nhắp chuột vào đường liên kết đó thì Storm Worm sẽ ngay lập tức đột nhập vào PC của họ. Nó bắt đầu phát tán qua một bức thư điện tử có tiêu đề *"230 người chết khi một cơn bão quét qua châu Âu"* và sau đó được thay bằng nhiều tiêu đề gác như '*Tin xấu'* hay **Chiến tranh Thế giới thứ ba đã bắt đầu**. Virus này đã lây nhiễm rất nhanh với khoảng 10 triệu máy tính trở thành nạn nhân của nó.

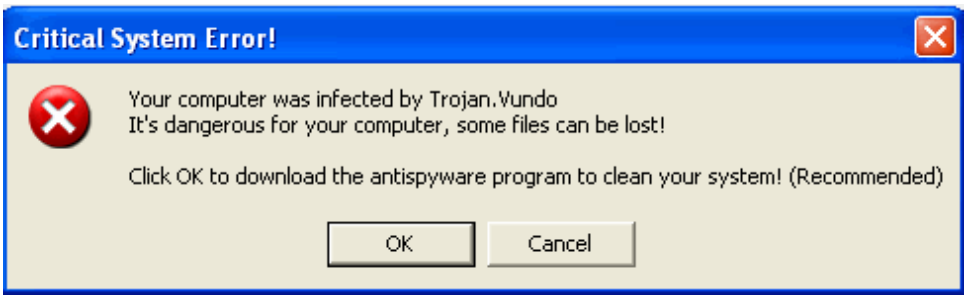
Trojan Horse

- Là một chương trình nguy hiểm thường trong diện mạo như là một chương trình hữu ích. Không giống như virus, nó không có chức năng tự sao chép nhưng lại có chức năng hủy hoại tương tự virus. Một trong những thứ giăng bẫy của Trojan Horse là nó tự nhận là giúp cho máy của thân chủ chống lại các virus nhưng thay vì làm vậy nó quay ra đem virus vào máy.
- Khác nhau căn bản với virus máy tính là Trojan Horse về mặt kỹ thuật chỉ là một phần mềm thông thường và không có ý nghĩa tự lan truyền. Các chương trình này chỉ lừa người dùng để tiến hành các thao tác khác mà thân chủ sẽ không tự nguyện cho phép tiến hành. Ngày nay, các Trojan horse đã được thêm vào đó các chức năng tự phân tán. Điều này đẩy khái niệm Trojan horse đến gần với khái niệm virus và chúng trở thành khó phân biệt.
- Người tấn công có thể đính kèm một Trojan horse vào một cái tên có vẻ lương thiện vào trong một thư điện tử với việc khuyến dụ người đọc mở đính kèm ra. Các biểu tượng cũng có thể được gán với các loại tệp khác nhau và có thể được đính kèm vào thư điện tử. Khi người dùng mở các biểu tượng này thì các Trojan horse ẩn giấu sẽ tiến hành những tác hại bất ngờ và Lợi dụng một số lỗi của trình duyệt web, chẳng hạn như Internet Explorer, để nhúng Trojan vào một trang web, khi người dùng xem trang này sẽ bị nhiễm
- **Các kiểu gây hại rất nhiều điển hình bao gồm:**

1. Xoá hay viết lại các dữ liệu trên máy tinh
2. Làm hỏng chức năng của các tệp
3. Lây nhiễm các phần mềm ác tính khác như là virus
4. Cài đặt mạng để máy có thể bị điều khiển bởi máy khác hay dùng máy nhiễm để gửi thư nhũng lạm
5. Đọc lén các thông tin cần thiết và gửi báo cáo đến nơi khác
6. Ăn cắp thông tin như là mật khẩu và số thẻ tín dụng
7. Đọc các chi tiết tài khoản ngân hàng và dùng vào các mục tiêu phạm tội

8. Cài đặt lén các phần mềm chưa được cho phép

- Vundo là loại Trojan horse điển hình. Nó tạo ra nhiều quảng cáo popup để quấy rối những chương trình chống spyware, làm suy giảm khả năng thực thi của hệ thống và cản trở trình duyệt web. Đặc biệt, nó cản trở cài đặt chương trình quét malware trực tiếp đĩa CD.



Virus (máy tính)

- Nằm trong khái niệm malware rộng lớn, Virus được xem là một dạng phổ biến nhất. Virus tồn tại dưới dạng được cài đặt và ẩn nấp sau các chương trình khác (Malware). No sẽ được lây lan và phá hoại sau khi malware xâm nhập vào được hệ thống máy tính của bạn. Ngoài ra, nó cũng có thể tồn tại riêng lẻ ở dạng những chương trình con hay những đoạn mã chương trình được thiết kế để thực hiện tối thiểu là hai việc:

  1. Tự xen vào hoạt động hiện hành của máy tính một cách hợp lệ, để thực hiện tự nhân bản và những công việc theo chủ ý của người lập trình. Sau khi kết thúc thực thi mã virus thì điều khiển được trả cho trình đang thực thi mà máy không bị "treo", trừ trường hợp virus cố ý treo máy.
  2. Tự sao chép chính nó, tức tự nhân bản, một cách hợp lệ lây nhiễm vào những tập tin (file) hay các vùng xác định (boot, FAT sector) ở các thiết bị lưu trữ như đĩa cứng, đĩa mềm, thiết bị nhớ flash (phổ biến là USB),... thậm chí cả EPROM chính của máy.

- Virus thường lây lan qua các phần mềm bẻ khóa, các phần mềm sao chép lậu, các thiết bị nhớ di động, mạng nội bộ, mạng Internet, đặc biệt là thư điện tử, các lỗ hổng hệ điều hành và phần mềm,…

- Tác hại thường thấy của Virus máy tính là Tiêu tốn tài nguyên hệ thống, Phá hủy dữ liệu, Phá hủy hệ thống, Đánh cắp dữ liệu, Mã hóa dữ liệu để tống tiền, Gây khó chịu khác,..

- Mới đây nhất là con virus cực kỳ nguy hiểm có tên là Wannacry. WannaCry là một dạng phần mềm *"tống tiền"(ransomware)* theo phương thức khóa các dữ liệu trên máy tính của người dùng, sau đó mã hóa chúng khiến người sử dụng không thể truy cập các dữ liệu đó được nữa. Wannacry có thể xâm nhập vào máy tính của người dùng, sau đó tìm kiếm kết nối thêm với các máy tính khác để lan truyền mã độc càng nhiều càng tốt.

Nói tóm lại. Dù là Virus, Trojan Horse hay Worm, thì chúng đều là các phần mềm độc hại, và không ít thì nhiều, chúng đều có tác động, ảnh hưởng trực tiếp đến hiệu quả hoạt động cũng như "thời gian sống" của chiếc máy tính của bạn.

CÁCH PHÒNG CHỐNG VIRUS VÀ NGĂN CHẶN TÁC HẠI CỦA NÓ

- **Sử dụng phần mềm diệt Virus**
- **Sử dụng tường lửa cá nhân**

  -Sử dụng tường lửa bằng phần cứng

  -Sử dụng tường lửa bằng phần mềm
- **Cập nhật các bản vá lỗi của hệ điều hành**
- **Vận dụng kinh nghiệm sử dụng máy tính**

  -Phát hiện sự hoạt động khác thường của máy tính

  -Kiểm soát các ứng dụng đang hoạt động

  -Loại bỏ một số tính năng tự động của hệ điều hành

  -Quét virus trực tuyến
- **Bảo vệ dữ liệu máy tính**

  -Sao lưu dữ liệu theo chu kỳ

  -Tạo các dữ liệu phục hồi cho toàn hệ thống