# Module 7
# VIRUS VÀ WORM

## Những Nội Dung Chính Trong Chương Này

*Sự Khác Biệt Giữa Virus Và Worm*

*Phân Loại Virus*

*Dò Tìm Và Gỡ Bỏ Virus*


Virus máy tính có lẽ là thuật ngữ được nhiều người biết đến nhất trong lĩnh vực an toàn thông tin, kèm theo đó là những ngộ nhận giữa virus máy tính và virus gây tác hại đối với con người. Tôi còn nhớ rất rõ hình ảnh một người bạn học đã dùng khăn lau sạch chiếc để mềm trước khi cho vào máy vi tính để đề phòng virus hay có nhiều cơ quan vào những năm đầu của thập niên 90 đã yêu cầu các nhân viên phải bỏ dép bên ngoài khi vào phòng máy chủ. Vậy virus máy tính là gì ? Về mặt tác hại đối với máy tính thì cũng tương tự như đối với con người đó là làm cho hệ thống máy hoạt động mất ổn định, bị hư hỏng, bị xóa tập tin hay thậm chí gây gãy đổ toàn hệ thống. Chúng có khả năng lây lan trên mạng Lan và mạng internet thông qua các lổ hỗng bảo mật hay do sự bất cẩn của người dùng, do thiếu các giải pháp phòng ngừa cẩn thận.

Nhiều virus máy tính còn mang theo các trojan hay backdoor cho phép hacker đột nhập vào hệ thống hay truy cập dữ liệu trái phép. Một trong virus có tốc độ lây lan chóng mặt là conflicker đã gây ra các cơn bão dữ liệu trên mạng internet, làm tràn ngập mạng LAN khiến cho nhiều hoạt động bị tê liệt.

# Sự Khác Biệt Giữa Virus Và Worm

Virus và Worm đều là những phần mềm nguy hiểm gây thiệt hại về mặt kinh tế hay phá hũy dữ liệu của người dùng. Theo thống kê hàng năm mỗi người dân thiệt hại hơn một triệu VND (tổng thiệt hại cả nước trong năm 2010 do virus và sâu máy tính khoảng 5900 tỉ đồng – theo số liệu khảo sát của BKAV) do các tác động mà virus đem lại, nếu như tính cả chi phí phải bỏ ra để mua những phần mềm diệt virus thì số thiệt hại này có lẽ còn lớn hơn nhiều. Tuy nhiên, về mặt cơ bản thì giữa chúng có những khác biệt cơ bản mà các bạn cần phân biệt trong các câu hỏi hay tình huống nêu ra ở  kì thi chứng chỉ CEH đó là bản thân các chương trình virus không tự mình lây lan mà chỉ nhiễm vào các ứng dụng có khả năng thực thì, sau đó lây lên các máy tính khác khi người dùng sao chép hay di chuyển những tập tin này bằng USB, email hay trò chơi điện tử ... Trong khi đó Worm hay sâu máy tính có thể tự mình tìm kiếm những điểm yếu của các máy tính khác ở trên mạng để lây nhiễm. Morris là sâu máy tính đầu tiên xuất hiện trên mạng internet vào ngày 2 tháng 11 năm 1988 từ học viện MIT, còn các thế hệ sâu máy tính ngày nay thường tấn công vào các mạng xã hội ví dụ như sâu máy tính lan truyền qua mạng Twitter.

# Phân Loại Virus

Virus được phân loại dựa trên đối tượng và cách thức mà chúng lây nhiễm. Một virus máy tính có thể lây nhiễm vào các thành phần sau đây của hệ thống :

- System sector

- Tập tin
- Macros (như MS Word macro)
- Các tập tin hay hàm thư viên của hệ thống như DLL, INI
- Disk cluster
- Tập tin BAT
- Mã nguồn ứng dụng

Và để lây nhiễm vào những thành phần trên thì các virus cần có sự tác động từ bên ngoài như các hành động sao chép, *download* và thực thi chương trình của người dùng. Sau đây là các loại virus được phân chia theo cách thức lây lan của chúng :

- **Polymorphic** là loại virus mã hóa mã nguồn của chúng theo nhiều cách khác nhau để qua mặt chương trình dò tìm.
- **Stealth** là virus che dấu các đặc điểm nhận dạng của chúng như thay đổi thời gian mà tập tin được tạo để ngăn không cho các chương trình antivirus phát hiện có những tập tin mới trên hệ thống.
- **Fast & Slow Infector** là dạng virus sử dụng cơ chế lây lan thật nhanh hay thật chậm để tránh bị phát hiện.
- **Armored** là loại virus sử dụng các kỹ thuật mã hóa để tránh bị dò tìm.
- **Multipartie** là một loại virus cao cấp có thể chia tiến trình lây nhiễm thành nhiều giai đoạn.
- **Cavity (space-filler)** các virus dạng này tự chèn chúng vào các phần trống của tập tin.
- **Tunneling** là virus được gởi thông qua những giao thức hay được mã hóa để ngăn ngừa sự phát hiện cũng như qua mặt firewall.
- **Camouflage** là dạng virus giả danh như là một chương trình khác nhằm đánh lừa người sử dụng.
- **NTFS & Active Directory** các virus dạng này chuyên tấn công vào các hệ thống tập tin NTFS của Windows hay tấn công trực tiếp vào Active Directory.

Các chuyên gia bảo mật thường ví cơ sở dữ liệu nhận dạng dựa trên các *signature* (chữ kí) như là "*máu*" của các chương trình diệt virus. Vì vậy, hacker đã tìm cách viết

ra các kịch bản hay virus xóa đi các đặc trưng nhận dạng của chúng nhằm qua mặt các ứng dụng antivirus, trong trường hợp này các ứng dụng quét virus phải sử dụng cơ chế nhận dạng dựa trên hành vi để phát hiện các hoạt động bất thường của chương trình nguy hiểm.

Cũng như các biện pháp phòng chống trojan / backdoor để bảo vệ và phòng chống bị lây nhiễm virus chúng ta cần sử dụng  các chương trình quét virus mạnh được cập nhật đầy đủ. Không sử dụng các chương trình thiêu tin cậy như bản crack, chương trình patch hay những phần mềm trôi nỗi trên mạng internet. Nên quét virus  và thường xuyên. Cập nhật đầy đủ các bản vá hệ thống để hạn chế không cho chương trình nguye hiểm và các hacker khai thac từ xa.

## Dưới Đây Là Các Bước Dò Tìm Và Gỡ Bỏ Virus

1. Dò tìm các hành vi bất thường của hệ thống như các cảnh báo lỗi, tìm kiếm trong event view…

2. Dò tìm các tiến trình với những công cụ như pslist.exe, fport.exe, netstat.exe … nhằm phát hiện các dịch vụ bất thường trên hệ thống.

3. Dò tìm các payload của virus trên các tập tin bị nhiễm hay bị thay thế.

4. Cô lập các thành phần bị nhiễm để tránh sự lây lan sang các hệ thống khác và tiến hành quét virus các hệ thống này trên những chương trình diệt virus được cập nhật đây đủ.

Các bạn có thể tham khảo thêm một số bài giảng về virus thuộc chương trình CEH tại http://youtu.be/-Cw2XQQAQFw (giới thiệu virus máy tính) hay http://youtu.be/0JAWQuLDXBM (tạo virus bằng công cụ).

# Tổng Kết

Trong chương này các bạn đã tìm hiểu về virus và worm, mỗi loại có những điểm khác biệt đặc trưng nhưng cả hai đều là các ứng dụng gây ảnh hưởng đến sự vận hành của hệ thống một khi bị lây nhiễm. Vì vậy chúng ta cần có các biện pháp phòng tránh cũng như áp dụng quy trình diệt thích hợp để nâng cao tính an toàn cho hệ thống. Nguồn gốc của sự lây nhiễm virus hay worm thường do máy tính hay chương trình thiếu các bản cập nhật hay bản vá lỗi, cài đặt và sử dụng các chương trình không có nguồn gốc rõ ràng cũng như bất cẩn trong việc thiết lập các chính sách an ninh, và trên hết các bạn cần nâng cao nhận thức về an toàn thông tin cho người dùng, đặc biệt là kiến thức về virus và sâu máy tính.