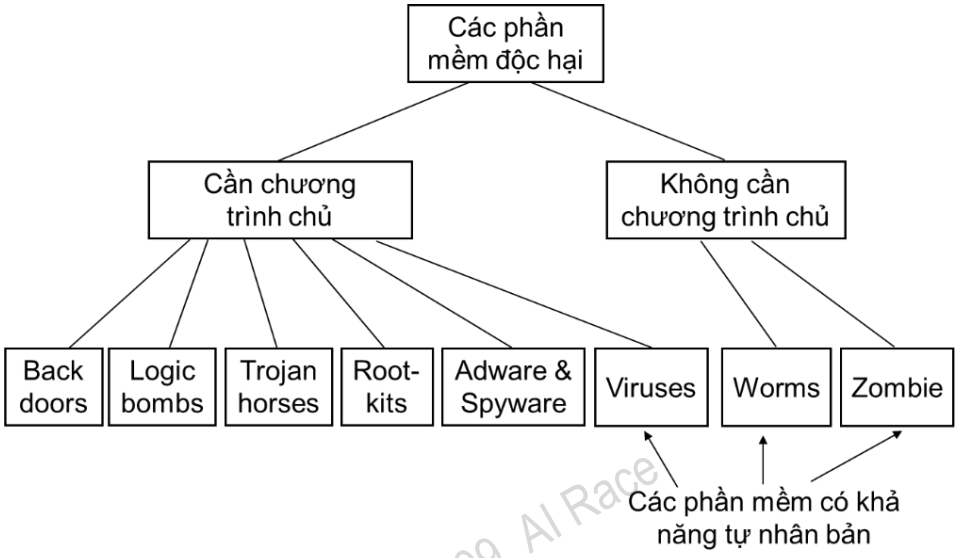
1. Giới thiệu

Các phần mềm độc hại (Malware hay Malicious software) là các chương trình, phần mềm được viết ra nhằm các mục đích xấu, như đánh cắp thông tin nhạy cảm, hoặc phá hoại các hệ thống. Có nhiều phương pháp phân loại các phần mềm độc hại, trong đó một phương pháp được thừa nhận rộng rãi là chia các phần mềm độc hại thành 2 nhóm chính như biểu diễn trên Hình 2.33:

- Các phần mềm độc hại cần chương trình chủ, vật chủ (host) để ký sinh và lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Logic bomb (Bom logic), Back door (Cửa hậu), Trojan horse (Con ngựa thành Tơ roa), Virus (Vi rút), Rootkit, Adware (Phần mềm quảng cáo) và Spyware (Phần mềm gián điệp).
- Các phần mềm độc hại không cần chương trình chủ, vật chủ để lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Worm (Sâu) và Zombie hay Bot (Phần mềm máy tính ma).

Trong số các phần mềm độc hại, các phần mềm độc hại có khả năng tự lây nhiễm (self-infection), hay tự nhân bản (self-replicate) gồm Vi rút, Sâu và Phần mềm máy tính ma. Các dạng còn lại không có khả năng tự lây nhiễm. Việc phân loại các phần mềm độc hại kể trên mang tính chất tương đối do hiện nay, có một số phần mềm độc hại có các đặc tính của cả Vi rút, Sâu và Phần mềm gián điệp.



Hình 2.33. Các dạng phần mềm độc hại

2. Các dạng phần mềm độc hại

2.1 Logic bomb

Logic bomb (Bom lô gíc) là các đoạn mã độc thường được "nhúng" vào các chương trình bình thường và thường hẹn giờ để "phát nổ" trong một số điều

kiện cụ thể. Điều kiện để bom "phát nổ" có thể là sự xuất hiện hoặc biến mất của các file cụ thể, một thời điểm cụ thể, hoặc một ngày trong tuần. Khi "phát nổ" bom logic có thể xoá dữ liệu, file, tắt cả hệ thống...

Thực tế đã ghi nhận quả bom logic do Tim Lloyd cài lại đã "phát nổ" tại công ty Omega Engineering vào ngày 30/7/1996, 20 ngày sau khi Tim Lloyd bị sa thải. Bom lô gíc này đã xoá sạch các bản thiết kế và các chương trình, gây thiệt hại 10 triệu USD cho công ty. Bản thân Tim Lloyd bị phạt 2 triệu USD và 41 tháng tù.

2.2 Trojan Horse

Trojan horse lấy tên theo tích "Con ngựa thành Tơ roa", là chương trình chứa mã độc, thường giả danh những chương trình có ích, nhằm lừa người dùng kích hoạt chúng. Trojan horse thường được sử dụng để thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập. Chẳng hạn, trong một hệ thống nhiều người dùng, một người dùng (kẻ tấn công) có thể tạo ra một trojan đội lốt một chương trình hữu ích đặt ở thư mục chung. Khi trojan này được thực thi bởi một người dùng khác, nó sẽ thay đổi quyền truy nhập các file và thư mục của người dùng đó, cho phép tất cả người dùng (trong đó có kẻ tấn công) truy nhập vào các file của người dùng đó.

2.3 Back door

Back door (Cửa hậu) thường được các lập trình viên tạo ra, dùng để gỡ rối và kiểm thử chương trình trong quá trình phát triển. Cửa hậu thường cho phép truy nhập trực tiếp vào hệ thống mà không qua các thủ tục kiểm tra an ninh thông thường. Khi cửa hậu được lập trình viên tạo ra để truy nhập bất hợp pháp vào hệ thống, nó trở thành một mối đe dọa đến an ninh hệ thống. Cửa hậu thường được thiết kế và cài đặt khéo léo và chỉ được kích hoạt trong một ngữ cảnh nào đó, do vậy nó rất khó bị phát hiện.

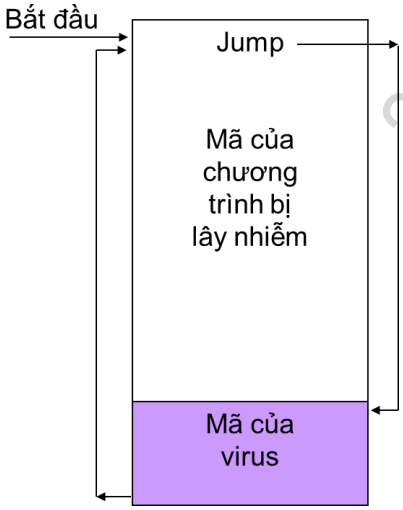
2.4 Virus

2.4.1 Giới thiệu

Hình 2.34. Minh họa vi rút máy tính

Vi rút (Virus) là một chương trình có thể "nhiễm" vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu các chương trình đã bị sửa đổi chứa vi rút được kích hoạt thì vi rút sẽ tiếp tục "lây nhiễm" sang các chương trình khác. Tương tự như vi rút sinh học, vi rút máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc. Có nhiều con đường lây nhiễm vi rút, như sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email...

Vi rút có thể thực hiện được mọi việc mà một chương trình thông thường có thể thực hiện. Khi đã lây nhiễm vào một chương trình, vi rút tự động được thực hiện khi chương trình này chạy. Hình 2.35 minh họa việc chèn mã vi rút vào cuối một chương trình và chỉnh sửa chương trình để khi chương trình được kích hoạt, mã vi rút luôn được thực hiện trước, sau đó mới thực hiện mã chương trình.



Hình 2.35. Chèn và gọi thực hiện mã vi rút

2.4.2 Các loại vi rút

Các loại vi rút thường gặp bao gồm file vi rút, boot vi rút, macro vi rút và email vi rút. Boot vi rút là dạng vi rút lây nhiễm vào cung khởi động (boot sector) của đĩa hoặc phần hệ thống của đĩa như cung khởi động chủ của đĩa cứng (master boot record). Do boot vi rút lây nhiễm vào cung khởi động nên nó luôn được nạp vào bộ nhớ mỗi khi hệ thống máy khởi động. Boot vi rút có thể gây hỏng phần khởi động của đĩa, thậm chí có thể làm cho đĩa không thể truy nhập được.

File vi rút là dạng vi rút phổ biến nhất, đối tượng lây nhiễm của chúng là các file chương trình và các file dữ liệu. Mỗi khi chương trình được kích hoạt hoặc file dữ liệu được nạp vào bộ nhớ, vi rút được kích hoạt. Mọi chương trình tiếp theo được kích hoạt đều bị lây nhiễm vi rút này. File vi rút có thể làm hỏng chương trình, hỏng hoặc phá hủy các file dữ liệu, đánh cắp các dữ liệu nhạy cảm,…

Macro vi rút là một loại file vi rút đặc biệt do chúng chỉ lây nhiễm vào các tài liệu của bộ phần mềm Microsoft Office. Macro vi rút hoạt động được nhờ tính năng cho phép tạo và thực hiện các đoạn mã macro trong các tài liệu của bộ ứng dụng Microsoft Office, gồm ứng dụng soạn thảo Word, bảng tính Excel, trình email Outlook,…. Các đoạn mã macro thường được dùng để tự động hóa 1 số việc và được viết bằng ngôn ngữ Visual Basic for Applications (VBA). Macro vi rút thường lây nhiễm vào các file định dạng chuẩn (các template như normal.dot và normal.dotx) và từ đó lây nhiễm vào tất cả các file tài liệu được mở. Macro vi rút cũng có thể được tự động kích hoạt nhờ các auto- executed macros, như AutoExecute, Automacro và Command macro. Theo thống kê, macro vi rút chiếm khoảng 2/3 tổng lượng vi rút đã được phát hiện. Lượng tài liệu bị lây nhiễm macro vi rút đã giảm đáng kể từ khi Microsoft Office 2010 có

thiết lập ngầm định không cho phép tự động chạy các macro.

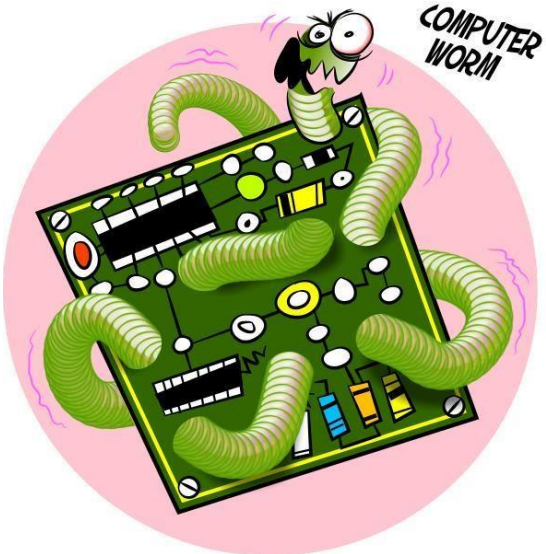
Email vi rút lây nhiễm bằng cách tự động gửi một bản copy của nó như 1 file đính kèm đến tất cả các địa chỉ email trong sổ địa chỉ của người dùng trên máy bị lây nhiễm. Nếu người dùng mở email hoặc file đính kèm, vi rút được kích hoạt. Email vi rút có thể lây nhiễm rất nhanh chóng, lan tràn trên khắp thế giới trong một thời gian ngắn.

2.5 Worm

Worm (Sâu) là một loại phần mềm độc hại có khả năng tự lây nhiễm từ máy này sang máy khác mà không cần chương trình chủ, vật chủ, hoặc sự trợ giúp của người dùng. Khi sâu lây nhiễm vào một máy, nó sử dụng máy này làm "bàn đạp" để tiếp tục rà quét, tấn công các máy khác. Một trong các dạng sâu phổ biến là *sâu mạng* (network worm) sử dụng kết nối mạng để lây lan từ máy này sang máy khác. Mặc dù sử dụng phương thức lây lan khác vi rút, khi sâu hoạt động, nó tương tự vi rút.

Sâu có thể lây lan sử dụng nhiều phương pháp khác nhau. Một số sâu chỉ sử dụng một phương pháp lây lan, nhưng một số sâu khác có khả năng lây lan theo nhiều phương pháp. Các phương pháp lây lan chính của sâu gồm:

- Lây lan qua thư điện tử: Sâu sử dụng email để gửi bản sao của mình đến các máy khác.
- Lây lan thông qua khả năng thực thi từ xa: Sâu gửi và thực thi một bản sao của nó trên một máy khác thông qua việc khai thác các lỗ hổng an ninh của hệ điều hành, các dịch vụ, hoặc phần mềm ứng dụng.
- Lây lan thông qua khả năng log-in (đăng nhập) từ xa: Sâu đăng nhập vào hệ thống ở xa như một người dùng và sử dụng lệnh để sao chép bản thân nó từ máy này sang máy khác.



Hình 2.36. Minh họa sâu máy tính

Sâu Code Red được phát hiện vào tháng 7/2001 lây nhiễm thông qua việc khai thác lỗi tràn bộ đệm khi xử lý các file .ida trong máy chủ web Microsoft IIS (Internet Information Service). Code Red quét các địa chỉ IP ngẫu nhiên để tìm các hệ thống có lỗi và lây nhiễm vào 360.000 máy chủ trong vòng 14 giờ. Sau đó, sâu Nimda được phát hiện vào tháng 9/2001 là sâu có khả năng lây lan theo nhiều con đường:

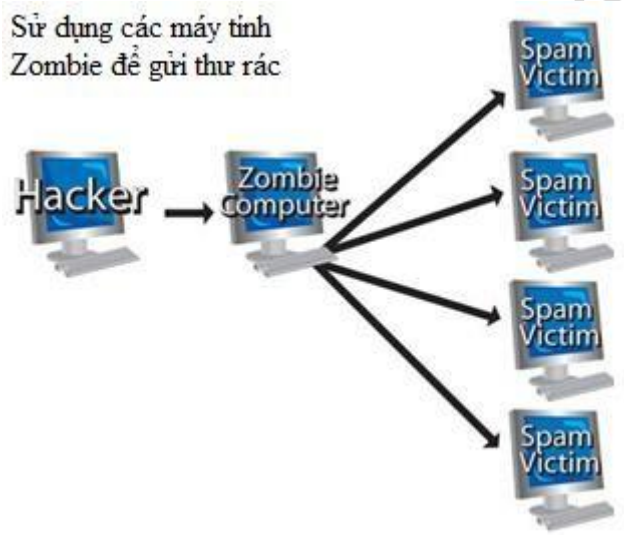
- Qua email từ máy client sang client.
- Qua các thư mục chia sẻ trên mạng.
- Từ máy chủ web sang trình duyệt.
- Từ máy khách đến máy chủ nhờ khai thác các lỗi máy chủ.

Chỉ 22 phút sau khi ra đời, Nimda trở thành sâu có tốc độ lan truyền nhanh nhất trên Internet vào thời điểm đó.

2.6 Zombie

Zombie (còn gọi là *Bot* hoặc *Automated agent*) là một chương trình được thiết kế để giành quyền kiểm soát một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để tấn công các hệ thống khác, hoặc gửi spam email. Tương tự như sâu, zombie có khả năng tự lây nhiễm sang các hệ thống khác mà không cần chương trình chủ, hoặc các hỗ trợ từ người dùng. Một tập hợp các máy tính zombie/bot dưới sự kiểm soát của một, hoặc một nhóm tin tặc được gọi là mạng máy tính ma, hay zombie network/botnet. Các zombie thường được điều phối và sử dụng để thực hiện các cuộc tấn công DDoS các máy chủ, các website của các công ty, hoặc các tổ chức chính phủ. Các máy tính zombie cũng có

thể được sử dụng để gửi thư rác tạo ra khoản tiền không nhỏ cho các nhóm tin tặc, như minh họa trên Hình 2.37.



Hình 2.37. Mô hình tin tặc sử dụng các máy tính Zombie để gửi thư rác

2.7 Rootkit

Rootkit là một dạng phần mềm độc hại gồm một tập các công cụ có mục đích giành quyền truy nhập vào hệ thống máy tính mà người dùng không có thẩm quyền không thể truy nhập. Rootkit thường che giấu mình bằng cách đội lột một phần mềm khác. Rootkit có thể được cài đặt tự động, hoặc tin tặc cài đặt rootkit khi chiếm được quyền quản trị hệ thống. Do rootkit có quyền truy nhập hệ thống ở mức quản trị nên nó có toàn quyền truy nhập vào các thành phần trong hệ thống và rất khó bị phát hiện.

2.8 Adware và Spyware

Adware (tên đầy đủ là advertising-supported software) là các phần mềm tự động hiển thị các bảng quảng cáo trong thời gian người dùng tải hoặc sử dụng các phần mềm. Adware thường được đóng gói chung với các phần mềm khác có thể dưới dạng như một phần của một phần mềm hoặc một dịch vụ miễn phí. Adware trong một số trường hợp có thể được coi là một phần mềm độc hại nếu chúng được tự động cài đặt và kích hoạt mà không được sự đồng ý của người dùng.

Spyware là một dạng phần mềm độc hại được cài đặt tự động nhằm giám sát, thu thập và đánh cắp các thông tin nhạy cảm trên hệ thống nạn nhân. Có 4 loại spyware thường gặp, gồm system monitor (giám sát hệ thống), trojan, adware, and tracking cookies (các cookie theo dõi). Spyware có thể được cài đặt vào hệ thống nạn nhân thông qua nhiều phương pháp, như tích hợp, đóng gói vào các phần mềm khác, bẫy nạn nhân tự tải và cài đặt, hoặc tin tặc có thể sử dụng vi rút, sâu để tải và cài đặt. Spyware thường được trang bị khả năng ẩn mình nên rất khó có thể phát hiện bằng các phương pháp thông thường.