TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

\*

BÁO CÁO

**NHẬP MÔN CNTT**

NGÀNH CÔNG NGHỆ THÔNG TIN

CHỦ ĐỀ: AN TOÀN THÔNG TIN

PHÂN BIỆT CÁC KHÁI NIỆM VIRUS, TROJAN, WORM

Nhóm sinh viên thực hiện: Trần Tuấn Minh 20215618

Phan Trọng Cường 20215538

Ngô Đình Luyện 20215419

Hoàng Đức Huy 20215392

Nguyễn Đức Hiếu 20215370

Lớp KSTN Khoa học Máy tính – K66

Giáo viên hướng dẫn: Nguyễn An Hưng

Trợ giảng hướng dẫn: Trương Văn Hiển

HÀ NỘI – 2021

**NỘI DUNG THUYẾT TRÌNH**

[**I. Giới thiệu về malware** 3](#_Toc86052099)

[1. Khái niệm 3](#_Toc86052100)

[2. Các cách xâm nhập của malware và các loại malware phổ biến 3](#_Toc86052101)

[**II. Virus** 3](#_Toc86052102)

[1. Khái niệm 3](#_Toc86052103)

[2. Cơ chế hoạt động 3](#_Toc86052104)

[3. Đặc điểm một số loại virus thường gặp 4](#_Toc86052105)

[**III. Trojan** 4](#_Toc86052106)

[1. Khái niệm 4](#_Toc86052107)

[2. Cơ chế hoạt động 4](#_Toc86052108)

[3. Đặc điểm 5](#_Toc86052109)

[**IV. Worm** 5](#_Toc86052110)

[1. Khái niệm 5](#_Toc86052111)

[2. Cơ chế hoạt động 6](#_Toc86052112)

[3. Đặc điểm 6](#_Toc86052113)

[**V. Tổng hợp, so sánh** 7](#_Toc86052114)

# **I. Giới thiệu về malware**

## **1. Khái niệm**

Malware (hay phần mềm độc hại) là thuật ngữ mô tả các chương trình hoặc mã độc có khả năng cản trở hoạt động bình thường của hệ thống bằng cách xâm nhập, kiểm soát, làm hỏng hoặc vô hiệu hóa hệ thống mạng, máy tính, [máy tính bảng](https://www.thegioididong.com/may-tinh-bang) và [thiết bị di động](https://www.thegioididong.com/dtdd),…

## **2. Các cách xâm nhập của malware và các loại malware phổ biến**

***a) Các cách xâm nhập của malware***

* Truy cập các trang web độc hại, tải trò chơi, file nhạc nhiễm Malware, cài đặt thanh công cụ/phần mềm từ nhà cung cấp lạ, mở tệp đính kèm [email](https://www.thegioididong.com/game-app/gmail-cua-google-gui-email-nhanh-chong-220098) độc hại (malspam) hoặc các dữ liệu tải xuống không được quét bởi phần mềm bảo mật.
* Tải nhầm các ứng dụng độc hại ngụy trang dưới dạng các ứng dụng hợp pháp, các thông báo cảnh báo khi cài đặt ứng dụng, đặc biệt khi ứng dụng yêu cầu quyền truy cập email hoặc thông tin cá nhân.
* Tải ứng dụng ở các nguồn không đáng tin cậy.
* Vô tình cài đặt các phần mềm bổ sung đi kèm với ứng dụng (potentially unwanted program) chứa Malware.
* Ngoài ra, việc không sử dụng các chương trình bảo mật cũng là lý do khiến Malware xâm nhập dễ dàng hơn.

***b) Một số loại malware phổ biến***

* Virus
* Trojan
* Worm
* Rootkit
* Ransomware

Trong bài thuyết trình này, chúng ta chỉ tìm hiểu về 3 loại chính là Virus, Trojan, Worm.

# **II. Virus**

## **1. Khái niệm**

**Virus máy tính** hay còn thường được gọi là virus là **những đoạn mã chương trình** được thiết kế với mục đích nhằm**xâm nhập vào máy tính** người dùng từ đó lấy cắp các thông tin các nhân, xóa dữ liệu hay thậm chí là gửi email nặc danh và có thể tự nhân bản và sao chép chính nó vào các chương trình khác.

## **2. Cơ chế hoạt động**

Máy tính được thiết kế hoạt động bằng các lệnh ở dạng**mã máy** là các dãy số nhị phân và được lập trình dẫn tới những công việc được xác định lặp đi lặp lại nhiều lần để tổ chức thành **module riêng gọi là "trình con"**trong ngôn ngữ lập trình gọi là **routine**, khi thực hiện tác vụ cho routine thì trình đang chạy thực hiện lệnh đến routine đó để thực thi một tác vụ nhất định nào đó mà người dùng yêu cầu. Virus được**viết dưới dạng một routine**, sẽ  thực hiện**sửa tham số địa chỉ** của một số lệnh trỏ đến địa chỉ của nó. Khi kết thúc virus thì chuyển điều khiển đến routine được gọi của trình.

## **3. Đặc điểm một số loại virus thường gặp**

* Browser Hijacking : Loại virus này chiếm quyền một vài chức năng của trình duyệt web. Khi bật trình duyệt web chúng có thể tự động bật một trang web được hacker cài sẵn.
* Virus thường trú/Resident virus: Biến thể virus này có khả năng tự chèn vào bộ nhớ của hệ thống máy tính. Virus thường trú có thể được thực thi bất cứ lúc nào khi hệ điều hành của bạn khởi động.
* Virus đa hình/ Polymorphic virus: Loại virus này rất khó phòng chống vì có khả năng tránh các chương trình chống virus. Đặc điểm của virus máy tính là chúng sẽ thay đổi mã của nó mỗi khi tệp bị nhiễm được thực thi.
* Virus nạp tập tin/File infector virus: Loại virus khá phổ biến vì có thể chèn mã độc vào các tệp thực thi để thực hiện các chức năng, các hoạt động nhất định trên hệ thống máy tính của bạn.
* Virus đa phân/Multipartite virus: Loại virus có thể lây nhiễm và lây lan theo nhiều cách khác nhau. Nó có thể lây nhiễm cả các tệp chương trình hoặc cả các khu vực trong hệ thống máy tính của bạn.
* Virus macro: Loại virus này có khả năng sẽ lây lan khi bạn vô tình mở một tài liệu hoặc click vào link bị nhiễm virus, thường thông là qua tệp đính kèm email.

# **III. Trojan**

## **1. Khái niệm**

Trojan (hay Trojan horse), trước hết là một chương trình độc hại cho máy tính, được ngụy trang bằng một vỏ bọc tưởng chừng vô hại để tạo tin tưởng cho người dùng, từ đó sử dụng và vô tình máy tính bị nhiễm trojan, bị thu thập mọi dữ liệu từ bên thứ 3 để phục vụ cho mục đích xấu là đánh cắp thông tin.

Trojan được lấy từ điển tích con ngựa thành Troia trong thần thoại Hy Lạp. Nội dung điển tích kể về sự thông minh của người Hy Lạp khi đã ẩn nấp vô số chiến binh trong thân con ngựa gỗ khổng lồ, khiến kẻ địch lầm tưởng đó là chiến tích thu được mà chủ quan, giúp quân Hy Lạp chiếm thành dễ dàng. Điều này cũng giống như cách thức hoạt động của trojan.

## **2. Cơ chế hoạt động**

Khởi đầu, trojan ẩn mình dưới rất nhiều hình thức khác nhau từ bài hát, phần mềm, hình ảnh, link tải, quảng cáo và lúc này diện mạo của chúng nhìn có vẻ an toàn, hợp pháp để người dùng tải xuống máy tính hay chỉ cần click chuột vào. Ngaysau đó, các phần mềm gián điệp sẽ nhanh chóng xâm nhập vào hệ thống máy tính, chờ tín hiệu của người muốn xâm nhập máy tính và sau đó tạo ra một cửa hậu để hắn khống chế toàn bộ dữ liệu cá nhân của người dùng.

Ví dụ, ngựa trojan có thể ẩn mã của nó trong một hình thức đăng nhập bằng cách đính kèm với nó. Khi người dùng chèn chi tiết, trojan sẽ gửi thông tin này cho kẻ tấn công mà không có kiến ​​thức của người dùng. Sau đó, kẻ tấn công có thể sử dụng các chi tiết người dùng để có quyền truy cập vào hệ thống.

Sau đây là những hoạt động phổ biến mà Trojan sẽ gây hại lên hệ thống máy tính của người dùng bị nhiễm:

* Xoá hay viết lại các dữ liệu trên máy tính.
* Làm hỏng chức năng của các tệp.
* Lây nhiễm các phần mềm ác tính khác như là virus.
* Đọc lén các thông tin cần thiết và gửi báo cáo đến nơi khác.
* Ăn cắp thông tin như là mật khẩu và số thẻ tín dụng.
* Cài đặt lén các phần mềm chưa được cho phép.

Khác với virus khi tấn công trực tiếp dễ bị phần mềm antivirus phát hiện, thì trojan tấn công dưới một chương trình, phần mềm khác như đuôi .exe,.com,.scr,.bat, hay.pif. Bên cạnh đó, Trojan là một phần mềm thông thường và không tự lây lan như virus.

## **3. Đặc điểm**

Một số loại trojan đơn giản khi xâm nhập máy tính để lại một số dấu hiệu nhận biết tới người dung như:

* Ổ CD-ROM tự động mở ra đóng vào.
* Dấu hiệu lạ trên màn hình máy tính.
* Hình nền máy tính tự động bị thay đổi.
* Các văn bản tự động in.
* Máy tính tự động thay đổi font chữ và các thiết lập khác.
* [Lỗi chuột máy tính](https://quantrimang.com/cach-khac-phuc-chuot-khong-hoat-dong-tren-windows-164259) như không hiển thị chuột, 2 chuột lẫn lộn nhau.
* Nút Start không hiển thị.
* Cửa sổ chat hiển thị mà không phải do bạn mở lên.

Tất nhiên đây chỉ là một vài dấu hiệu nhận biết cho những loại trojan đơn giản. Hiện nay trojan đã tinh vi hơn khi chúng không để lại bất cứ dấu hiệu nào, và ở nhiều dạng khác nhau. Và nếu có thời gian sau này chúng ta sẽ có thể tiếp tục tìm hiểu thêm.

# **IV. Worm**

## **1. Khái niệm**

Worm máy tính là một loại chương trình phần mềm độc hại có chức năng chính là lây nhiễm sang các máy tính khác trong khi vẫn hoạt động trên những hệ thống bị nhiễm.

Worm máy tính là phần mềm độc hại tự sao chép để lây lan sang các máy tính chưa bị nhiễm.Với tốc độ lây lan cực nhanh, chúng có khả năng tự nhân đôi để lây lan sang các [máy tính](https://fptshop.com.vn/may-tinh-xach-tay) chưa bị nhiễm trong cùng một mạng bằng cách tự động xâm nhập vào hệ điều hành và "vô hình" đối với người dùng. Thông thường, sâu máy tính chỉ được phát hiện khi chúng chiếm dụng quá nhiều tài nguyên hệ thống khiến mọi thứ bị chậm lại hoặc các tác vụ không thể sử dụng được nữa.

## **2. Cơ chế hoạt động**

Worm máy tính thường dựa vào các lỗi bảo mật và lỗ hổng trong các giao thức mạng để lan truyền giữa các máy tính. Nó sử dụng một máy làm máy chủ để quét và lây nhiễm cho các máy khác. Worm máy tính lây lan mà không cần có sự tương tác của người dùng , quá trình lây lan của sâu máy tính là một quá trình độc lập tự sao chép. Tất cả những gì cần thiết là để worm máy tính hoạt động trên hệ thống bị nhiễm.

Sau khi một con worm máy tính bắt đầu xâm nhập vào một hệ thống máy tính, nó thường cố gắng tồn tại hoạt động trên hệ thống càng lâu càng tốt. Lúc này nó sẽ tự động sao chép và lây lan sang nhiều hệ thống nhất có thể.

## **3. Đặc điểm**

***a) Sâu morris – Sâu đầu tiên xuất hiện***

Sâu Morris là [sâu máy tính](https://vi.wikipedia.org/wiki/S%C3%A2u_m%C3%A1y_t%C3%ADnh) đầu tiên được phát tán qua [Internet](https://vi.wikipedia.org/wiki/Internet); nó cũng là con sâu đầu tiên thu hút được sự chú ý đáng kể của các phương tiện thông tin đại chúng. Cha đẻ của nó là [Robert Tappan Morris](https://vi.wikipedia.org/w/index.php?title=Robert_Tappan_Morris&action=edit&redlink=1), một sinh viên 23 tuổi tốt nghiệp ngành khoa học máy tính tại [Đại học Cornell](https://vi.wikipedia.org/wiki/%C4%90%E1%BA%A1i_h%E1%BB%8Dc_Cornell). Sâu Morris được thả lên mạng vào ngày [2 tháng 11](https://vi.wikipedia.org/wiki/2_th%C3%A1ng_11) năm [1988](https://vi.wikipedia.org/wiki/1988) từ học viện [MIT](https://vi.wikipedia.org/wiki/H%E1%BB%8Dc_vi%E1%BB%87n_C%C3%B4ng_ngh%E1%BB%87_Massachusetts), nó được phát tán từ [MIT](https://vi.wikipedia.org/wiki/H%E1%BB%8Dc_vi%E1%BB%87n_C%C3%B4ng_ngh%E1%BB%87_Massachusetts) để che giấu thực tế là con sâu đã được bắt nguồn từ Cornell.

Sai lầm nghiêm trọng đã biến con sâu từ chỗ một thí nghiệm trí thức có tiềm năng vô hại thành một tấn công [từ chối dịch vụ](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5) đầy phá hoại do nhầm lẫn trong cơ chế lây lan.

***b)*** [***MyDoom - sâu phát tán nhanh nhất lịch sử máy tính***](https://vnexpress.net/so-hoa/hon-1-trieu-may-tinh-toan-cau-bi-nhiem-mydoom-1508913.html)

MyDoom, là một sâu máy tính chuyên tấn công vào hệ điều hành Microsoft Windows, được phát hiện lần đầu tiên vào ngày 26/01/2004 và là một sâu máy tính lan truyền rộng và nhanh nhất từ trước đến nay.

Nó được thiết kế như một thông điệp báo lỗi khiến người dùng cả tin bấm vào, vô tình biến họ thành spammer gửi thư rác tới tất cả những địa chỉ email có trong hòm thư.

***c) Wanna Cry – Sâu chiếm tài liệu tống tiền***

WannaCry (tạm dịch Muốn khóc) là một biến thể của mã độc tống tiền (ransomware), còn có tên gọi khác là WannaCrypt0r 2.0 hay WCry, bắt đầu bùng phát trên toàn thế giới từ ngày 11/5/17. Ransomware nguy hiểm bởi chúng "hiểu" dữ liệu của người dùng luôn quan trọng và việc giữ dữ liệu làm "con tin" sẽ có hiệu quả hơn là chỉ đánh cắp hoặc xóa đi.

***d) Một số loại sâu khác:***

Worm bot có thể được sử dụng để lây nhiễm vào máy tính và biến chúng thành zombie hoặc bot, với mục đích sử dụng chúng trong các cuộc tấn công.

Worm IM lan truyền thông qua các dịch vụ nhắn tin tức thời và khai thác quyền truy cập vào danh sách liên hệ trên máy tính người dùng.

# **V. Tổng hợp, so sánh**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Virus | Worm | Trojan |
| Xâm nhập thông qua | Lây qua mạng nội bộ, qua email, qua các tập tin tải về hay từ ổ đĩa USB. | Xâm nhập nhờ tận dụng điểm yếu của hệ thống hoặc ứng dụng | Đính kèm chính nó vào một chương trình và ngụy trang là một phần mềm hữu ích |
| Khả năng nhân bản | Có | Có | Không |
| Điều khiển từ xa | Không | Có | Có |
| Khả năng lan truyền | Vừa phải | Nhanh hơn | Chậm |
| Mục tiêu | Làm thay đổi thông tin | Ăn tài nguyên | Đánh cắp thông tin |