ĐẠI HỌC BÁCH KHOA HÀ NỘI

TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

──────── \* ───────

BÁO CÁO

**NHẬP MÔN CNTT**

NGÀNH CÔNG NGHỆ THÔNG TIN

**TÌM HIỂU VỀ VIRUS, TROJAN, WORM**

Nhóm sinh viên thực hiện: **Nhóm 6**

|  |  |
| --- | --- |
| **Nguyễn Đăng Dương**  **Vương Hoàng Minh**  **Phạm Hữu Bách**  **Phạm Đức Minh**  **Phạm Trung Hiếu** | – IT-TN K66 – 20215336  – IT-TN K66 – 20210590  – IT-TN K66 – 20210091  – IT-TN K66 – 20210586  – IT-TN K66 – 20214898 |

Giáo viên hướng dẫn: TS. **Nguyễn An Hưng**

HÀ NỘI T10-2021

**Bảng phân công công việc**

|  |  |
| --- | --- |
| **Họ và tên** | **Phân công** |
| Nguyễn Đăng Dương | Tổng hợp thông tin, làm báo cáo, thuyết trình |
| Vương Hoàng Minh | Tìm hiểu mã độc là gì, một số mốc thời gian đáng chú ý, cách phòng chống mã độc, thuyết trình |
| Phạm Hữu Bách | Tìm hiểu và thuyết trình về Trojan |
| Phạm Đức Minh | Tìm hiểu và thuyết trình về Virus |
| Phạm Trung Hiếu | Tìm hiểu và thuyết trình về Worm |

**MỤC LỤC**

[Lời nói đầu 3](#_Toc86505202)

[Chương 1: Tìm hiểu chung 4](#_Toc86505203)

[1.1 Phần mềm mã độc (Malware) là gì? 4](#_Toc86505204)

[1.2. Lịch sử 4](#_Toc86505205)

[Chương 2: Virus 5](#_Toc86505206)

[2.1. Virus là gì? 5](#_Toc86505207)

[2.2. Phương thức phát tán, tấn công 5](#_Toc86505208)

[2.3. Tác hại của Virus 5](#_Toc86505209)

[Chương 3: Trojan 6](#_Toc86505210)

[3.1. Trojan là gì? 6](#_Toc86505211)

[3.2. Phương thức phát tán, tấn công 6](#_Toc86505212)

[3.3. Thiệt hại 6](#_Toc86505213)

[Chương 4: Worm 7](#_Toc86505214)

[4.1. Worm là gì? 7](#_Toc86505215)

[4.2. Phương thức phát tán, tấn công 7](#_Toc86505216)

[4.3. Tác hại của Worm 7](#_Toc86505217)

[Chương 5: Các cuộc tấn công quy mô lớn 8](#_Toc86505218)

[**5.1. ILOVEYOU** 8](#_Toc86505219)

[a) ILOVEYOU là gì? 8](#_Toc86505220)

[b) Phương thức phát tán, tấn công 8](#_Toc86505221)

[c) Thiệt hại 9](#_Toc86505222)

[**5.2. WannaCry 9**](#_Toc86505223)

[a) WannaCry là gì? 9](#_Toc86505224)

[b) Phương thức phát tán, tấn công 9](#_Toc86505225)

[c) Thiệt hại 10](#_Toc86505226)

[Chương 6: Bảo mật thông tin 10](#_Toc86505227)

[6.1. Thực trạng tấn công mạng 10](#_Toc86505228)

[6.2. Một số biện pháp phòng chống Malware 11](#_Toc86505229)

[Chương 7: Kết luận 12](#_Toc86505230)

[Phụ lục 13](#_Toc86505231)

# Lời nói đầu

Trong thời đại bùng nổ của công nghệ thông tin và truyền thông, Internet đã trở thành một phần quan trọng trong cuộc sống của con người. Đặc biệt, dưới tác động của dịch Covid-19, thời gian người dùng bỏ ra để lên mạng đã tăng lên theo cấp số nhân. Tuy nhiên, mạng Internet luôn tiềm ẩn những mối nguy hại tiềm tang như các cuộc tấn công bảo mật bằng Virus, mã độc. Theo Báo cáo Rủi ro Toàn cầu (GRR), an ninh mạng và bất bình đẳng kĩ thuật số là vấn đề đáng lưu tâm thứ 5 của các quốc gia năm 2021. Quan tâm đến vấn đề này, chúng tôi – nhóm 6 – đã thu thập và tìm hiểu các phân loại mã độc đáng quan tâm, thiệt hại mà chúng gây ra cũng như cách phòng chống. Sau đây là báo cáo của chúng tôi.

# Chương 1: Tìm hiểu chung

## 1.1 Phần mềm mã độc (Malware) là gì?

**Phần mềm mã độc** (tiếng Anh: malware được ghép từ malicious và software) là một loại **phần mềm hệ thống** do các tay tin tặc (hacker) tạo ra nhằm **gây hại** cho các máy tính.

Tùy theo cách thức mà hacker sử dụng, sự nguy hại của các loại mã độc có thể khác nhau từ chỗ chỉ hiển thị các cửa sổ hù dọa cho đến việc đánh cắp dữ liệu quan trọng, tấn công chiếm quyền điều khiển và lây lan sang các máy tính khác.

Các loại Malware chính bao gồm: Virus, Trojan, Worm, Rootkits,…

## 1.2. Lịch sử

**Năm 1949:** John von Neumann (1903-1957) phát triển nền tảng lý thuyết tự nhân bản của 1 chương trình cho máy tính.

**Năm 1981:** Các virus đầu tiên xuất hiện trong hệ điều hành của máy tính Apple II.

**Năm 1983:** Tại Đại học miền Nam California - Hoa Kỳ, Fred Cohen lần đầu đưa ra khái niệm "Virus máy tính" (*computer virus*) như định nghĩa ngày nay.

**Năm 1986:** Virus "the Brain", virus cho máy tính cá nhân (PC) đầu tiên, được tạo ra tại Pakistan bởi Basit và Amjad.

**Năm 1990:** Phần mềm chống mã độc đầu tiên được phát triển dành cho dòng máy Mac ra đời.

**Hiện nay:** Các chương trình mã độc ngày càng xuất hiện nhiều, tinh vi hơn, nguy hiểm hơn; yêu cầu các chương trình chống mã độc phải ngày càng an toàn, bảo mật.

# Chương 2: Virus

## 2.1. Virus là gì?

**Virus** là các **đoạn code độc hại** được cài vào các file chương trình máy tính.

Khi chương trình hoạt động, các đoạn code này tiến hành quá trình **nhân bản** khiến các file khác trở thành bản sao của chính nó.

## 2.2. Phương thức phát tán, tấn công

Virus có ba phương pháp lây lan chính:

* **Kết nối vật lý:** ví dụ như USB, đĩa mềm, ổ cứng, đĩa CD,...
* **Qua Email:** Khi người dung mở những tệp, đường link khả nghi trong thử điện tử, Virus sẽ được tải về và lây nhiễm. Một vài trường hợp, kẻ phát tán lợi dụng lỗi bảo mật khiến máy tính nhiễm Virus ngay khi mở thư.
* **Qua Internet:** Virus thường nằm trên các file được lưu trữ đám mây hoặc các trang web độc hại.

Cách thức tấn công của Virus thực chất là quá trình tự nhân bản chính mình. Khi người dùng mở một file chứa Virus, chúng sẽ sao chép mã độc của chính mình cài vào cái file khác khiến các file này cũng bị lây nhiễm. Quá trình này sẽ tiếp diễn liên tục nếu người dùng không xóa hết toàn bộ các file chứa Virus.

## 2.3. Thiệt hại

Virus có khả năng tự nhân bản bản thân và ghi đè lên dữ liệu quan trọng của các file bị lây nhiễm. Vì vậy một cuộc tấn công Virus sẽ dẫn đến sự mất mát dữ liệu quy mô lớn. Nếu các máy tính của các phòng ban quốc gia, ngân hàng bị nhiễm Virus thì thiệt hại là vô cùng nặng nề.

# Chương 3: Trojan

## 3.1. Trojan là gì?

**Trojan** (hay Trojan horse), là một **chương trình độc hại** được **ngụy trang** bằng một vỏ bọc tưởng chừng vô hại để người dùng tin tưởng và sử dụng trong khi bí mật thực hiện những tác vụ không mong muốn theo động cơ của kẻ phát tán.

## 3.2. Phương thức phát tán, tấn công

Trojan thường được đính kèm trong thư điện tử, dụ người đọc tải về. Một vài kẻ xấu lợi dụng các lỗ hổng bảo mật của trình duyệt mạng để nhúng mã độc vào các trang web. Khi người dùng truy cập các trang web này, Trojan sẽ được tự động tải về máy.

Trojan thường không có khả năng tự khởi động hay tự nhân bản. Tuy nhiên, chúng thường có đuôi định dạng đáng tin như: .exe, .com, .bat,… nên thoát được kiểm duyệt của các chương trình bảo mật. Khi Trojan được khởi động, chúng sẽ bí mật thực hiện các tác vụ như: thu thập thông tin, theo dõi hoạt động người dùng,…

Ngày nay, một số Trojan được trang bị thêm khả năng tự lây lan khiến hai khái niệm Virus và Trojan trở nên khó phân biệt.

## 3.3. Thiệt hại

* Đánh cắp thông tin quan trọng của hệ thống.
* Theo dõi hoạt động của người dùng.
* Tải xuống các phần mềm độc hại khác.
* Vô hiệu hóa tác vụ hệ thống để tống tiền.

# Chương 4: Worm

## 4.1. Worm là gì?

**Sâu máy tính** (Worm) 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.

## 4.2. Phương thức phát tán, tấn công

Worm đôi khi được coi là một loại Virus đặc biệt do có cách thức phát tán, tấn công của chúng khá tương đồng. Tuy nhiên, Worm có thể tự sao chép bản thân mà không cần sự can thiệp của người dùng, và lây lan qua các máy tính khác thông qua các lỗ hổng bảo mật Internet hoặc các phương thức kết nối khác như USB hay đĩa mềm.

Worm thường giả dạng thành các phần tự động và vô hình với người dùng của hệ điều hành rồi tự nhân bản chính mình. Vì vậy, hầu hết Worm chỉ được chú ý khi sự sao chép của chúng trở nên mất kiểm soát gây lãng phí bộ nhớ và làm chậm hoặc dừng các tác vụ khác.

## 4.3. Tác hại của Worm

* Cài đặt thêm các phần mềm độc hại bổ sung.
* Thu thập dữ liệu cá nhân nhạy cảm.
* Ép các máy tính tham gia vào một cuộc tấn công Botnet – một cuộc tấn công bằng cách sử dụng các máy tính nhiễm Worm liên tục gửi yêu cầu đến một trang web hoặc hệ thống khiến mục tiêu không thể phản hồi kịp dẫn đến sụp đổ.
* Lây lan sang các máy tính khác với tốc độ khủng khiếp.

**Chương 5: Các cuộc tấn công quy mô lớn**

**5.1. ILOVEYOU**

**a) ILOVEYOU là gì?**

**ILOVEYOU** (hay Love Bug, Love pak) là **sâu máy tính** đã lây nhiễm cho hơn **chục triệu** máy tính cá nhân Window bắt đầu từ ngày 5 tháng 5 năm 2000.

**Thủ phạm:** Onel de Guzman (24 tuổi) một sinh viên người Philippines.

**Mục đích:** Ban đầu, Guzman đặt giới hạn để Virus chỉ lây lan ở Manila nhằm đánh cắp tài khoản, mật khẩu của người dân để có thể truy cập Internet. Theo lời khai, anh đã gỡ bỏ giới hạn để Virus lây lan trên toàn thế giới vì tò mò.

**b) Phương thức phát tán, tấn công**

* + - File chứa virus ILOVEYOU sẽ được đính kèm vào một email dưới dạng là một “bức thư tình”. File của bức thư tên là LOVE-LETTER-FOR-YOU.TXT.vbs.
    - Khi tải file về máy, Windows sẽ ẩn đi đuôi định danh .vbs và chỉ hiện ra là LOVE-LETTER-FOR-YOU.TXT. Vì vậy, người dùng lầm tưởng rằng đó chỉ là một tệp văn bản thông thường và mở nó ra khiến các dòng mã độc của virus được thực thi.
    - Virus ILOVEYOU bắt đầu quá trình nhân bản của mình đến các file phổ biến thời bấy giờ là .doc, .jpg, .jpeg, .mp3, .mp2,...:
      * File gốc sẽ bị biến mất hoặc bị hidden.
      * Tạo ra một bản sao mới có tên tương tự file gốc nhưng có phần đuôi là .vbs và bên trong là những dòng mã độc.
      * File .vbs nhiễm virus có thể tiếp tục lây nhiễm tới các file mới chưa bị nhiễm nếu người dùng mở ra.
* Tên miền homepage ở Internet Explore của hệ điều hành bị thay thế bởi đường link dẫn đến một trang web độc hại và tự động tải về máy một mã độc khác, tên là WIN-BUGFIX.exe
* File WIN-BUGFIX.exe sẽ gửi Email có nội dung y như bức thư điện tử chứa virus ban đầu trong Outlook đến những địa chỉ ở trong phần contacts.

### c) Thiệt hại

* + - Lây nhiễm tới hơn chục triệu máy tính vào năm 2000 tương đương với gần 10% số lượng máy tính thời bấy giờ.
    - Tốc độ phát tán virus ILOVEYOU nhanh tới mức chỉ trong vòng 10 ngày có tận hơn 50 triệu thông báo lây nhiễm được báo cáo.
    - Virus ILOVEYOU gây thiệt hại lên đến 5.5-8.7 tỷ USD và tiêu tốn 10-15 tỷ USD để xóa bỏ.
    - Vào thời điểm bùng phát, Lầu Năm Góc và Cơ quan Tình báo Trung ương ở Mỹ đã phải tắt bỏ hệ thống thư điện tử của họ để tránh bị lây nhiễm

## 5.2. WannaCry

### a) WannaCry là gì?

**WannaCry** (hay WannaDecryptor 2.0) là một **phần mềm độc hại** tống tiền tự lan truyền trên các máy tính với hệ điều hành Microsoft Windows bắt đầu từ tháng 5 năm 2017.

Tính tới ngày 15 tháng 5 đã gây lây nhiễm trên 230.000 máy tính ở 150 quốc gia, yêu cầu thanh toán tiền chuộc từ 300 tới 600 Euro bằng bitcoin với 20 ngôn ngữ.

**Thủ phạm:** chưa được xác định. Tuy nhiên, nhiều sự tương đồng đã được xác định giữa đoạn code của WannaCry với một chương trình mã độc đã tấn công hãng phim Sony Pictures của nhóm tin tặc Lazarus.

### b) Phương thức phát tán, tấn công

* Chương trình khai thác lỗ hổng bảo mật Eternal Blue trên các hệ điều hành lỗi thời của Windows như Wins XP, Wins 7,…
* WannaCry được trang bị cơ chế tự động phát tán trên môi trường Internet. Khi chúng tìm được mục tiêu phù hợp, chương trình sẽ xâm nhập vào hệ thống và lây lan.
* Trước khi thực sự tấn công, WannaCry sẽ cố gắng kết nối đến một tên miền được nhóm tin tặc thiết kế như một công tắc an toàn nếu Virus trở nên mất kiểm soát. Nếu không thể liên kết với tên miền này, Virus sẽ bắt đầu tấn công hệ thống.
* Toàn bộ tập tin, dữ liệu của hệ thống sẽ bị Virus mã hóa bằng giao thức RSA 2048-bit vô cùng phức tạp khiến người dùng mất toàn bộ dữ liệu và chỉ có thể lấy lại bằng cách gửi tiền chuộc cho nhóm tin tặc.

### c) Thiệt hại

* Cuộc tấn công mã độc tống tiền ảnh hưởng đến nhiều bệnh viện NHS ở Anh.
* Nhà máy Nissan Motor Manufacturing UK, Tyne and Wear đã ngừng sản xuất sau khi chương trình này nhiễm vào một số hệ thống của họ
* Hơn 1.000 máy tính tại Bộ Nội vụ Nga, Bộ Khẩn cấp Nga và công ty viễn thông của Nga MegaFon bị kiểm soát bởi WannaCry.

# Chương 6: Bảo mật thông tin

## 6.1. Thực trạng tấn công mạng



Trong 3 tháng đầu năm 2021, Cục An toàn thông tin, Bộ TT&TT đã ghi nhận 1.271 vụ tấn công mạng vào các hệ thống thông tin tại Việt Nam, giảm 20% so với cùng kỳ Quý I/2020.

Mặc dù so với cùng kỳ quý I/2020, số vụ tấn công mạng có giảm 20%. Tuy nhiên, nếu tính từ đầu năm 2021 đến nay, số vụ tấn công mạng vẫn có xu hướng tăng nhẹ. Cụ thể, trong tháng 3/2021, Cục An toàn thông tin đã ghi nhận 491 vụ tấn công mạng, tăng 8,15% so với tháng 2/2021.

Phân tích của chuyên gia Trung tâm Giám sát an toàn không gian mạng (NCSC) thuộc Cục An toàn thông tin cho thấy các tổ chức, cá nhân tội phạm mạng vẫn đang tăng cường lợi dụng nhu cầu sử dụng mạng internet ngày một gia tăng do sự quan tâm của người dân tới thông tin tình hình dịch bệnh COVID-19. Vì thế, số cuộc tấn công Phishing và Malware vào các hệ thống của các nhóm tin tặc để lừa đảo, phá hoại và đánh cắp thông tin trái phép đã gia tăng.

Vì vậy, vấn đề bảo mật thông tin đang trở nên vô cùng cấp thiết.

## 6.2. Một số biện pháp phòng chống Malware

Biện pháp đơn giản, hữu hiệu nhất là ngăn chặn toàn bộ kết nối thông tin của máy tính với các thiết bị ngoại vi khác như: kết nối USB, kết nối Internet,… Đây là phương pháp hay được sử dụng nhằm bảo vệ các thông tin tối mật của các cá nhân, tổ chức hay quốc gia. Tuy nhiên, trong thời đại công nghệ số, rất khó để các máy tính cá nhân áp dụng biện pháp này.

Một số biện pháp khác dành cho máy tính cá nhân hơn bao gồm:

* + Cài đặt các phần mềm phòng chống mã độc như: BKAV, Kaspersky, Avast,… và thường xuyên cập nhật chúng để nhận được hỗ trợ tốt nhất từ nhà phát triển.
  + Sử dụng tường lửa cá nhân nhằm kiểm soát kết nối Internet của các ứng dụng trong máy tính.
  + Liên tục cập nhật các bản vá lỗi bảo mật của hệ điều hành.
  + Vận dụng kinh nghiệm khi sử dụng máy tính:
    - Phát hiện các hoạt động bất thường của máy tính. VD: Tốc độ vận hành thay đổi, xuất hiện các kết nối bất thường,….
    - Kiểm soát các ứng dụng đang hoạt động. Chú ý đến các ứng dụng thường khởi chạy, chiếm CPU bao nhiêu,…
    - Vô hiệu một số chức năng tự động của hệ điều hành.
    - Chỉ truy cập vào những tệp dữ liệu, trang web đáng tin.
* Chủ động bảo vệ các dữ liệu quan trọng:
* Sao lưu dữ liệu theo chu kì.
* Tạo các dữ liệu phục hồi cho hệ thống.

# Chương 7: Kết luận

* Các phần mềm mã độc càng ngày càng đa dạng và nguy hiểm hơn theo từng phút, từng giây.
* Các phân loại như Virus, Trojan hay Worm đang ngày càng phát triển và trở nên khó phân biệt
* Người dùng máy tính cần phải nâng cao cảnh giác và trang bị các kiến thức cần thiết để phòng tránh các phần mềm mã độc.

# Phụ lục

* Mã độc: <https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_%C3%A1c_%C3%BD>
* Virus: <https://vi.wikipedia.org/wiki/Virus_(m%C3%A1y_t%C3%ADnh)>
* Trojan: <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>
* Worm: <https://vi.wikipedia.org/wiki/S%C3%A2u_m%C3%A1y_t%C3%ADnh>
* Virus ILOVEYOU:
  + <https://vi.wikipedia.org/wiki/ILOVEYOU>
  + <https://www.youtube.com/watch?v=jDmTdPYT7KE>
* Vụ tấn công WannaCry: <https://vi.wikipedia.org/wiki/V%E1%BB%A5_t%E1%BA%A5n_c%C3%B4ng_c%E1%BB%A7a_WannaCry>
* Botnet: <https://vi.wikipedia.org/wiki/Botnet>