|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN MÔN HỌC**

**BẢO MẬT THÔNG TIN**

**KEYLOGGER**

SINH VIÊN THỰC HIỆN: **LÊ NGUYỄN THÀNH LONG**

MSSV: 1811060436 LỚP: 18DTHB3

**ĐẶNG PHƯỚC TÀI**

MSSV: 1811061015 LỚP: 18DTHB3

TP. HỒ CHÍ MINH, 04/2021

|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN MÔN HỌC**

**BẢO MẬT THÔNG TIN**

**KEYLOGGER**

NGÀNH: **CÔNG NGHỆ THÔNG TIN**

MÔN HỌC: **BẢO MẬT THÔNG TIN**

SINH VIÊN THỰC HIỆN: **LÊ NGUYỄN THÀNH LONG**

MSSV: 1811060436 LỚP: 18DTHB3

**ĐẶNG PHƯỚC TÀI**

MSSV: 1811061015 LỚP: 18DTHB3

GVHD: **THS. TỐNG THANH VĂN**

TP. Hồ Chí Minh, 04/2021

Mục Lục

[LỜI NÓI ĐẦU 1](#_Toc69997568)

[CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU 2](#_Toc69997569)

[1.1. Đánh giá thực trạng về đề tài nguyên cứu 2](#_Toc69997570)

[1.1.1. Khảo sát thực trạng 2](#_Toc69997571)

[1.1.2. Đánh giá 3](#_Toc69997572)

[1.1.3. Ưu điểm 3](#_Toc69997573)

[1.1.4. Nhược điểm 3](#_Toc69997574)

[1.2. Nhiệm vụ nghiên cứu 4](#_Toc69997575)

[1.2.1. Đối tượng và phạm vi của ứng dụng 4](#_Toc69997576)

[1.2.2. Mô tả phương án nghiên cứu 4](#_Toc69997577)

[1.3. Cấu trúc đồ án 4](#_Toc69997578)

[CHƯƠNG 2. CƠ CHẾ HOẠT ĐỘNG PHẦN MỀM KEYLOGER 5](#_Toc69997579)

[2.1. Các khái niệm 5](#_Toc69997582)

[2.1.1. Tổng quan về Visual Studio 5](#_Toc69997583)

[2.2. Cơ chế hoạt động 6](#_Toc69997584)

[CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM 7](#_Toc69997585)

[3.1. Các thành phần chức năng của hệ thống 7](#_Toc69997586)

[3.2. Ứng dụng thứ hỗ trợ 10](#_Toc69997587)

[CHƯƠNG 4. KẾT QUẢ NGHIÊN CỨU 11](#_Toc69997588)

[4.1. Kết quả đạt được 11](#_Toc69997589)

[4.2. Kết quả chưa đạt được 11](#_Toc69997590)

[4.3. Hướng phát triển và mở rộng đề tài 11](#_Toc69997591)

[4.5. Phân công công việc 11](#_Toc69997592)

[4.6. Tài liệu tham khảo 11](#_Toc69997593)

[Nhận Xét Của Giảng Viên 12](#_Toc69997594)

# LỜI NÓI ĐẦU

**Keylogger** hay "trình theo dõi thao tác bàn phím" theo cách dịch ra tiếng Việt là một chương trình máy tính ban đầu được viết nhằm mục đích theo dõi và ghi lại mọi thao tác thực hiện trên bàn phím vào một tập tin nhật ký (log) để cho người cài đặt nó sử dụng. Vì chức năng mang tính vi phạm vào riêng tư của người khác này nên các trình keylogger được xếp vào nhóm các phần mềm gián điệp.

Về sau, khi **Keylogger** phát triển cao hơn nó không những ghi lại thao tác bàn phím mà còn ghi lại cả các hình ảnh hiển thị trên màn hình (screen) bằng cách chụp (screen-shot) hoặc quay phim (screen-capture) thậm chí còn ghi nhận cách con trỏ chuột trên máy tính di chuyển.

Xuất phát từ những lý do trên, cùng với sự hướng dẫn của Giảng viên **Thạc Sĩ Tống Thanh Văn** , chúng em thực hiện đề tài “**Keylogger**” để vận dụng những kiến thức đã được học vào thực tiễn, xây dựng một ứng dụng giám sát.

Chúng em xin chân thành cảm ơn!

Sinh viên thực hiện

**Lê Nguyễn Thành Long**

**Đặng Phước Tài**

# CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU

## 1.1. Đánh giá thực trạng về đề tài nguyên cứu

### 1.1.1. Khảo sát thực trạng

Keylogger, thông thường là một phần mềm nhỏ gọn, tuy nhiên cũng có những trường hợp chúng là thiết bị phần cứng (sẽ cực kì nguy hiểm trong trường hợp này). Có khả năng ghi nhớ lại mọi phím bấm mà người dùng đã thực hiện ở trên bàn phím.

Sau đó Keylogger sẽ tổ hợp lại các tổ hợp phím đó để tìm ra được các thông tin cá nhân, nội dung tin nhắn trao đổi như email, skype, số thẻ tín dụng và những mật khẩu trên các website của người dùng, và coi như mình đã mất toàn bộ thông tin khi bị tấn công Keylogger vào tay kẻ xấu.

Keylogger, nếu phục vụ cho mục đích tốt thì chúng được sử dụng trong các tổ chức Công nghệ Thông tin (IT) nhằm phát hiện lỗ và tiến hành hắc phục sự cố kỹ thuật với máy tính và mạng lưới kinh doanh.

Đối với các hộ gia đình (có thể cả doanh nghiệp) thì chúng được sử dụng để theo hoạt động sử dụng mạng của các thành viên, đặc biệt trong gia đình có trẻ nhỏ, các phụ huynh sủ dụng chúng để giám sát nội dung truy cập mạng của con cái mình.

Với mục đích xấu: Cách sử dụng keylogger dưới tay của kẻ xấu, chúng biến thành công cụ rất nguy hiểm. Một khi Keylogger được cài vào trong máy tính của mình thì các thông tin cá nhân, mật khẩu, nội dung Internet, số thẻ tín dụng,….của mình đều sẽ bị lộ.

### 1.1.2. Đánh giá

Phụ thuộc vào các loại keylogger khác nhau thì chúng sẽ cho những khả năng khai thác khác nhau, nhưng thường thì chúng đều có thể khai thác được những thông tin sau đây:

* Ghi chép lại các mật khẩu mà người dùng đã từng nhập trên thiết bị.
* Tự động gửi báo cáo chứa các bản ghi được lưu trữ và gửi email đến một địa điểm từ xa thông qua email, FTP, HTTP.
* Thực hiện chụp ảnh màn hình thiết bị với một khoảng thời gian chu kì nhất định.
* Các ứng dụng mà người dụng chạy trên thiết bị đều được ghi lại.
* Chụp lại được cả các website người dùng đã từng truy cập, ghi lại chính xác các URL mà người dùng đã vào bằng trình duyệt.
* Chụp bản sao các email đã gửi.
* Chụp bản ghi của tất cả tin nhắn tức thời từ Zalo, Facebook Messenger, Skype, Viber,...

Keylogger không chỉ ghi lại các thao tác phím mà còn thực hiện chụp màn hình máy tính. Khi đã lấy được các thông tin về, Keylogger có thể lưu trữ dữ liệu ngay trên ổ cứng của người dùng hoặc chuyển ngay thông tin đó qua mạng về một máy tính được chỉ định từ xa khác (hoặc là một web server khác).

### 1.1.3. Ưu điểm

Đối với các hộ gia đình (có thể cả doanh nghiệp) thì chúng được sử dụng để theo hoạt động sử dụng mạng của các thành viên, đặc biệt trong gia đình có trẻ nhỏ, các phụ huynh sủ dụng chúng để giám sát nội dung truy cập mạng của con cái mình.

### 1.1.4. Nhược điểm

Cách sử dụng keylogger dưới tay của kẻ xấu, chúng biến thành công cụ rất nguy hiểm. Một khi Keylogger được cài vào trong máy tính của bạn thì các thông tin cá nhân, mật khẩu, nội dung Internet, số thẻ tín dụng,….của bạn đều sẽ bị lộ.

## 1.2. Nhiệm vụ nghiên cứu

### 1.2.1. Đối tượng và phạm vi của ứng dụng

#### 1.2.1.1. Đối tượng

Hệ thống Keylogger được xây dựng hướng đến những đối tượng sử dụng máy tính chạy hệ điều hành windows 10.

### 1.2.2. Mô tả phương án nghiên cứu

#### 1.2.2.1. Phương án lưu trữ

Lưu trữ trong thư mục “**ROOT”** của ứng dụng và thông tin của victim sẽ được gửi qua mail thông qua thời gian có thể tùy chỉnh.

#### 1.2.2.2. Phương án khả thi

Dễ làm, dễ thực hiện, dễ sử dụng và khó bị phát hiện nếu victim không để ý.

## 1.3. Cấu trúc đồ án

**CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU**

**CHƯƠNG 2: CƠ SỞ LÝ THUYẾT**

**CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM**

**CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU**

# CHƯƠNG 2. CƠ CHẾ HOẠT ĐỘNG PHẦN MỀM KEYLOGER



## 2.1. Các khái niệm

### 2.1.1. Tổng quan về Visual Studio



**Visual studio** là một trong những công cụ hỗ trợ [lập trình website](https://monamedia.co/dich-vu/thiet-ke-website/) rất nổi tiếng nhất hiện nay của Mcrosoft và chưa có một phần mềm nào có thể thay thế được nó. Visual Studio được viết bằng 2 ngôn ngữ đó chính là C# và VB+. Đây là 2 ngôn ngữ lập trình giúp người dùng có thể lập trình được hệ thống một các dễ dàng và nhanh chóng nhất thông qua Visual Studio.

Visual Studio là một phần mềm lập trình hệ thống được sản xuất trực tiếp từ [Microsoft](https://www.microsoft.com/vi-vn/). Từ khi ra đời đến nay, Visual Studio đã có rất nhiều các phiên bản sử dụng khác nhau. Điều đó, giúp cho người dùng có thể lựa chọn được phiên bản tương thích với dòng máy của mình cũng như cấu hình sử dụng phù hợp nhất.

Bên cạnh đó, Visual Studio còn cho phép người dùng có thể tự chọn lựa giao diện chính cho máy của mình tùy thuộc vào nhu cầu sử dụng.

## 2.2. Cơ chế hoạt động

Hook là kỹ thuật điều khiển thông điệp (message-handling) giúp cho ứng dụng có thể cài đặt một thủ tục để điều khiển luồng thông điệp và tiến hành xử lý các thông điệp đó trước khi thông điệp đó đi tới cửa sổ đích.

Hook có thể xem là tính năng mạnh mẽ nhất của Windows, nó cho phép ta đặt bẫy đối với các sự kiện. Bằng cách sử dụng hook, ta có thể điều hướng ứng dụng tới một thủ tục mới bất kể khi nào mà sự kiện được quan tâm xuất hiện và bất kể sự kiện đó thuộc tiến trình của bạn hay thuộc tiến trình khác.

Để viết được chương trình Hook ta cần nắm bắt cơ chế xử lý thông điệp của Windows, Thư viện Win32 API và Kỹ thuật Hook.

Một phần mềm gián điệp theo dõi bàn phím **Keylogger** được cài đặt trực tiếp hoặc gián tiếp vào máy tính. Quá trình cài đặt được diễn ra khi người sử dụng mở file dữ liệu đính kèm từ email, hoặc kích vào đường link có file chứa phần mềm gián điệp. Một **Keylogger** có kích thước nhỏ khoảng vài chục kilobyte và hoàn toàn có thể được nhúng vào bên trong các file nhạc MP3 hoặc các file văn bản. Vì vậy người sử dụng hoàn toàn không nhận biết được sự hiện diện của các phần mềm loại này trên máy tính của mình. Sau khi đã cài đặt trong máy, **Keylogger** thiết lập vị trí các thư mục, tập tin và các thông số cần thiết đảm bảo cho hoạt động. Khi chuyển sang giai đoạn hoạt động, **Keylogger** theo dõi các sự kiện của hệ gõ phím; ghi lại diễn biến vào một hoặc file nhật ký (log) tại các vị trí đã thiết lập. Tại công đoạn tiếp theo, **Keylogger** gửi các file log ra ngoài máy tính bị theo dõi thông qua các kết nối mạng như gửi thư điện tử, truyền file FTP, hoặc gửi nhận thông qua ứng dụng lập trình socket. Quá trình hoạt động Để thu thập được các thao tác gõ phím, phần mềm gọi ngắt Windows để bắt trực tiếp các thông tin từ bàn phím. Dữ liệu thu thập được sẽ được lưu trong file, và sau đó được gửi định kỳ ra ngoài bằng kỹ thuật lập trình socket TCP.

Các kỹ thuật được liệt kê như sau:

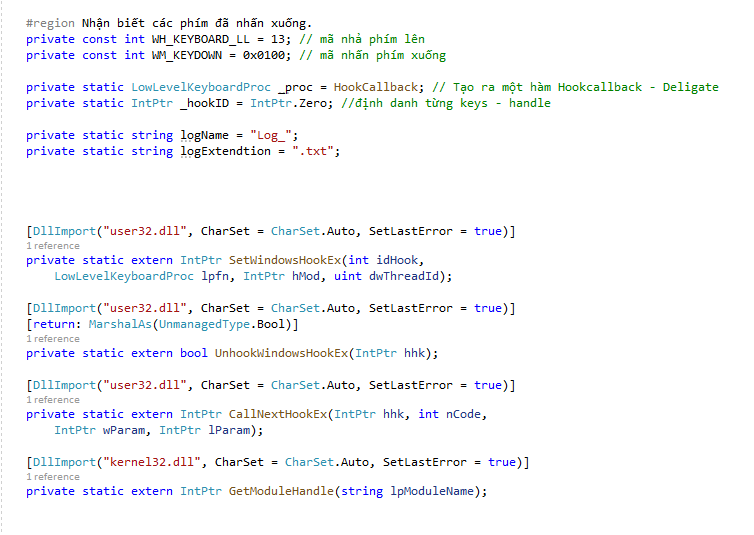
- Gọi ngắt bàn phím trong Windows để bắt các ký tự được nhập vào.

- Sử dụng các giao thức TCP/IP để truyền dữ liệu qua mạng.

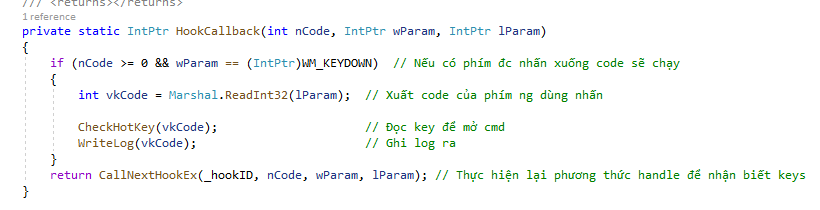
- Điều khiển phần mềm theo dõi

# CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM

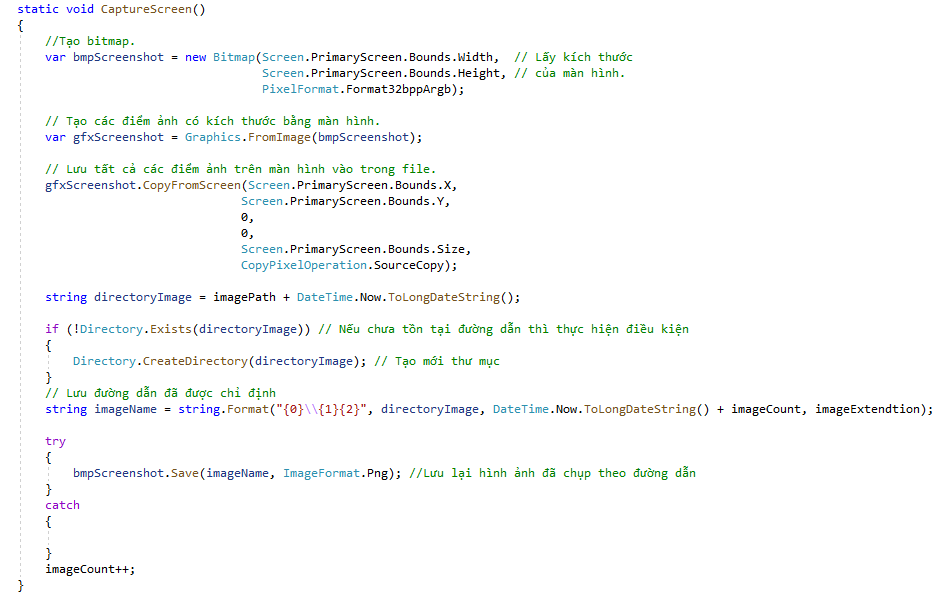
## 3.1. Các thành phần chức năng của hệ thống



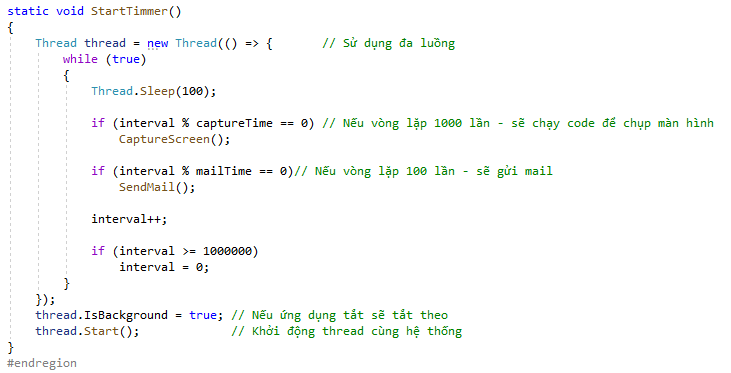
Hình 1 Hook Key



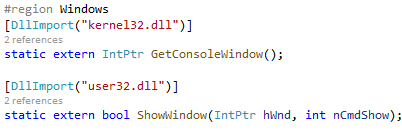
Hình 2 Hook Call Back



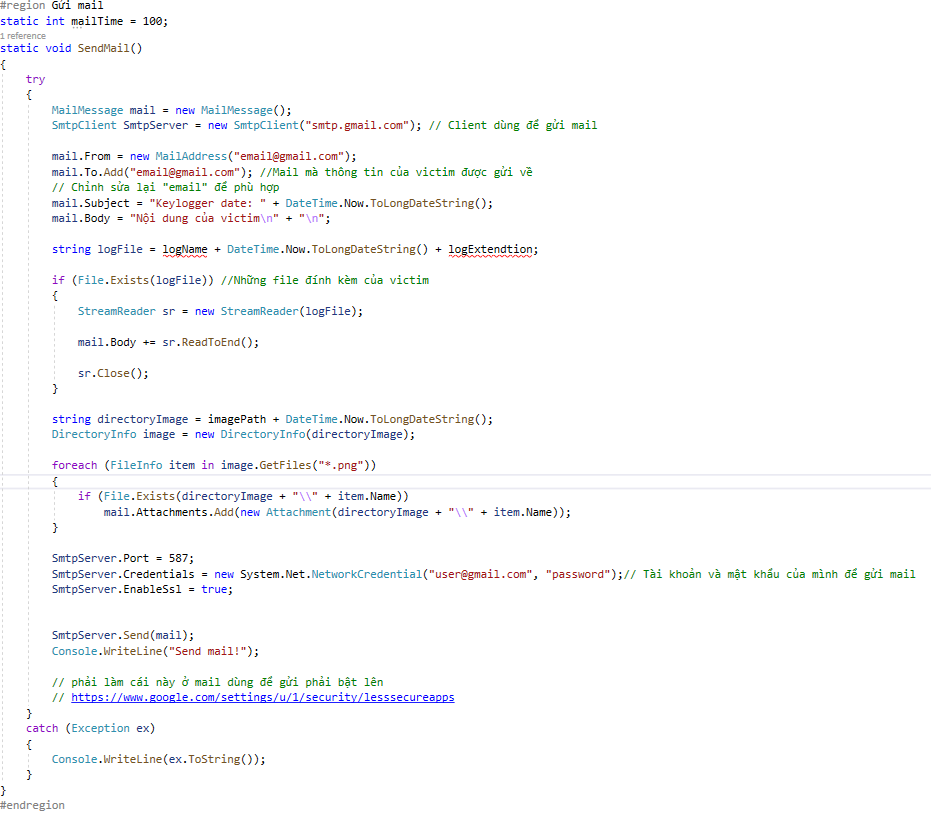
Hình 3 Capture Screen



Hình 4 Tinh chỉnh thời gian



Hình 5 Sử dụng thư viện của Windows



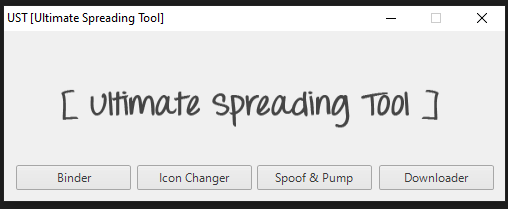
Hình 6 Code chụp màn hình



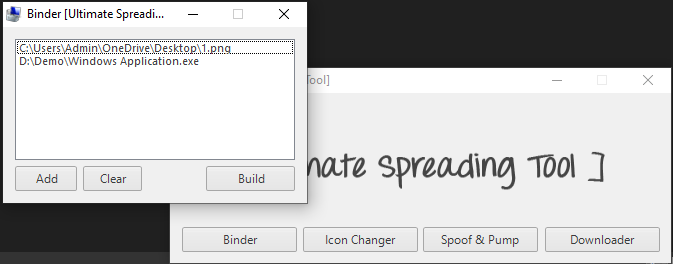
Hình 7 Tạo quyền registry và mở cùng windows

# 

## 3.2. Ứng dụng thứ hỗ trợ



Hình 8 Ứng dụng hỗ trợ đính kèm file



Hình 9 Đính kèm file vô một tệp khác

# CHƯƠNG 4. KẾT QUẢ NGHIÊN CỨU

## 4.1. Kết quả đạt được

Lấy được thông tin người dùng nhập từ bàn phím.

Lấy được hình ảnh màn hình người dùng trong khoảng thời gian có thể điều chỉnh.

Thông tin của victim được gửi qua mail được định sẵn.

Phần mềm chạy mỗi khi máy được mở lên.

## 4.2. Kết quả chưa đạt được

Chưa đổi được hình ảnh của file khi gửi cho người khác.

Chưa vượt được tường lửa.

## 4.3. Hướng phát triển và mở rộng đề tài

Thêm chức năng chiếm quyền điều khiển máy

Có thể quan sát theo thời gian thực

## 4.5. Phân công công việc

- Lê Nguyễn Thành Long (Nhóm trưởng):

+ Làm phần mềm

+ Tổng quan về word

- Đặng Phước Tài

+ Làm PowerPoint

## 4.6. Tài liệu tham khảo

<https://bit.ly/3tBtwPf> ( Thư viện của windows)

<https://bit.ly/3sOVfLj> ( Kiến thức cơ bản về Keylogger )

# Nhận Xét Của Giảng Viên

………………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….………………………………………………………………………………………………………….…………………………………………………………………………………………………………………………….

TP. HCM, ngày… tháng … năm 2021

**Giảng Viên Hướng Dẫn**