**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP.HCM**



**BÁO CÁO ĐỒ ÁN**

**BẢO MẬT THÔNG TIN**



**KEYLOGGER**

Ngành**:** **CÔNG NGHỆ THÔNG TIN**

Chuyên ngành: **CÔNG NGHỆ PHẦN MỀM**

Giảng viên hướng dẫn:

Lớp:

Sinh viên thực hiện:

|  |  |
| --- | --- |
|  |  |
|  |  |

Thành phố Hồ Chí Minh, năm 2022

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP.HCM**



**BÁO CÁO ĐỒ ÁN**

**BẢO MẬT THÔNG TIN**



**KEYLOGGER**

Ngành**:** **CÔNG NGHỆ THÔNG TIN**

Chuyên ngành: **CÔNG NGHỆ PHẦN MỀM**

Giảng viên hướng dẫn:

Lớp:

Sinh viên thực hiện:

|  |  |
| --- | --- |
|  |  |
|  |  |

Thành phố Hồ Chí Minh, năm 2022

# LỜI CẢM ƠN

Trước tiên với tình cảm sâu sắc và chân thành nhất, cho phép chúng em được bày tỏ lòng biết ơn đến tất cả thầy cô và nhà trường đã tạo điều kiện hỗ trợ, giúp đỡ chúng em trong suốt quá trình học tập và nghiên cứu đề tài này. Trong suốt thời gian từ khi bắt đầu học tập tại trường đến nay, chúng em đã nhận được rất nhiều sự quan tâm, giúp đỡ của quý Thầy Cô và bạn bè.

Với lòng biết ơn sâu sắc nhất, chúng em xin gửi đến quý Thầy Cô ở khoa Công Nghệ Thông Tin đã truyền đạt vốn kiến thức quý báu cho chúng em trong suốt thời gian học tập tại trường. Nhờ có những lời hướng dẫn, dạy bảo của các thầy cô nên đề tài nghiên cứu của chúng em mới có thể hoàn thiện tốt đẹp.

Một lần nữa, chúng em xin chân thành cảm ơn thầy Dương Minh Chiến – người đã trực tiếp giúp đỡ, quan tâm, hướng dẫn chúng em hoàn thành tốt bài báo cáo này trong thời gian qua.

Bài báo cáo thực hiện trong khoảng thời gian không nhiều bước đầu đi vào thực tế của chúng em còn hạn chế và còn nhiều bỡ ngỡ nên không tránh khỏi những thiếu sót. Chúng em rất mong nhận được những ý kiến đóng góp quý báu của quý Thầy Cô để kiến thức của chúng em trong lĩnh vực này được hoàn thiện hơn đồng thời có điều kiện bổ sung, nâng cao kiến thức của mình.

Chúng em xin chân thành cảm ơn!

Sinh viên thực hiện

# LỜI MỞ ĐẦU

Hiện nay lĩnh vực công nghệ thông tin đang ngày càng phát triển trên đất nước Việt Nam, ngày càng được ứng dụng rộng rãi trong các lĩnh vực của cuộc sống, đời sống xã hội. Việc hội nhập, tiếp thu kiến thức để áp dụng vào cuộc sống luôn là vấn đề được mọi tầng lớp quan tâm. Con người ngày càng sáng chế ra nhiều loại máy móc, phương tiện hữu ích để phục vụ cho con người, nhằm giảm đi công sức mà con người phải bỏ ra, giúp cho công việc đạt hiệu quả hơn, cùng với đó thì mạng Internet đã và đang trở nên phổ biến hơn. Nó đem lại cho con người một cách tiếp cận thông tin ngoài những lợi ích to lớn của mình, mạng internet nhiều mối nguy hiểm tiềm tàng như: bị đánh cắp thông tin, theo dõi người dùng,....Với một hệ thống mạng máy tính, việc đảm bảo an thống tránh khỏi các nguy cơ, hiểm họa đe dọa rất được chú trọng việc đảm bảo đó cần hợp nhiều biện pháp khác nhau. Trong bản báo các này, chúng em trình bày về đề tài: “Keylogger”.

Báo của nhóm em được chia thành 3 chương:

Chương 1: Tổng quan về Keylogger

Chương 2: Cơ sở lý thuyết của Keylogger

Chương 3: Kết quả thực nghiệm

# MỤC LỤC

[LỜI CẢM ƠN i](#_Toc107694511)

[LỜI MỞ ĐẦU ii](#_Toc107694512)

[MỤC LỤC iii](#_Toc107694513)

[DANH MỤC HÌNH ẢNH v](#_Toc107694514)

[CHƯƠNG 1. TỔNG QUAN VỀ KEYLOGGER 1](#_Toc107694515)

[1.1. Khái niệm Keylogger 1](#_Toc107694516)

[1.2. Lịch sử của Keylogger 1](#_Toc107694517)

[1.3. Phân loại Keylogger 1](#_Toc107694518)

[1.3.1. Keylogger phần cứng 1](#_Toc107694519)

[1.3.2. Keylogger phần mềm 1](#_Toc107694520)

[1.4. Lợi ích và tác hại của Keylogger 2](#_Toc107694521)

[1.4.1. Lợi ích 2](#_Toc107694522)

[1.4.2. Tác hại 2](#_Toc107694523)

[1.5. Một số Keylogger phổ biến và ứng dụng phổ biến của Keylogger 2](#_Toc107694524)

[1.5.1. Một số Keylogger phổ biến 2](#_Toc107694525)

[1.5.2. Các ứng dụng phổ biến của Keylogger 3](#_Toc107694526)

[1.5.1.1. Các ứng dụng tích cực 3](#_Toc107694527)

[1.5.1.2. Các ứng dụng tiêu cực 3](#_Toc107694528)

[CHƯƠNG 2. CƠ SỞ LÝ THUYẾT CỦA KEYLOGGER 4](#_Toc107694529)

[2.1. Cách thức hoạt động của Keylogger 4](#_Toc107694530)

[2.2. Keylogger được sử dụng để làm gì và có thể thu thập những gì 5](#_Toc107694531)

[2.2.1. Keylogger được sử dụng để làm gì 5](#_Toc107694532)

[2.2.1.1. Ví dụ về keylog hợp pháp 5](#_Toc107694533)

[2.2.1.2. Ví dụ về keylog bất hợp pháp 5](#_Toc107694534)

[2.2.2. Keylogger có thể thu thập những gì 6](#_Toc107694535)

[2.3. Cách phòng tránh và phát hiện và xử lý khi bị dính Keylogger 6](#_Toc107694536)

[2.3.1. Cách phòng tránh 6](#_Toc107694537)

[2.3.1.1. Phòng ngừa "được cài đặt” 6](#_Toc107694538)

[2.3.1.2. Phòng ngừa "bị cài đặt” 7](#_Toc107694539)

[2.3.2. Cách phát hiện Keylogger 7](#_Toc107694540)

[2.3.3. Cách xử lý khi bị dính Keylogger 8](#_Toc107694541)

[2.4. Ví dụ về một số cách để tìm và xóa Keylogger trên một số Keylogger phổ biến 9](#_Toc107694542)

[2.4.1. Easy Keylogger 9](#_Toc107694543)

[2.4.1.1. Cách tìm 9](#_Toc107694544)

[2.4.1.2. Cách diệt : (Lưu ý ở đây sẽ có nhiều cách diệt khỏi Process) 10](#_Toc107694545)

[2.4.2. Perfect Keylogger 10](#_Toc107694546)

[2.4.2.1. Cách tìm 10](#_Toc107694547)

[2.4.2.2. Cách diệt 11](#_Toc107694548)

[2.4.3. Active Keylogger 11](#_Toc107694549)

[2.4.3.1. Cách tìm 11](#_Toc107694550)

[2.4.3.2. Cách diệt 12](#_Toc107694551)

[CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM 13](#_Toc107694552)

[3.1. Yêu cầu chuẩn bị 13](#_Toc107694553)

[3.2. Ghi lại file của Keylogger 13](#_Toc107694554)

[KẾT LUẬN 16](#_Toc107694555)

[TÀI LIỆU THAM KHẢO 17](#_Toc107694556)

# DANH MỤC HÌNH ẢNH

[Hình 3.2.1 Giao diện của Keylogger 13](#_Toc107694557)

[Hình 3.2.2 Tạo file text 14](#_Toc107694558)

[Hình 3.2.3 Hệ thống ghi nhận file text 14](#_Toc107694559)

[Hình 3.2.4 Hệ thống ghi nhận lịch sử truy cập Website 15](#_Toc107694560)

# CHƯƠNG 1. TỔNG QUAN VỀ KEYLOGGER

## Khái niệm Keylogger

Keylogger là một phần mềm hoặc phần cứng được thiết kế để theo dõi mọi thao tác thực hiện trên bàn phím máy tính của người dùng, nó có khả năng ghi lại mọi phím bấm mà người dùng đã nhấn trên bàn phím, sau đó tổng hợp kết quả của các tổ hợp phím này, kẻ cài đặt keylogger có thể thu rất nhiều thông tin như tin nhắn cá nhân, nội dung email, số thẻ tín dụng, mật khẩu của người dùng.

## Lịch sử của Keylogger

Keylogger đã tồn tại trong rất nhiều năm qua. Lịch sử của Keylogger không thể biết chính xác. Người ta tin rằng nó được xuất hiện đầu tiên bởi chính phủ và không biết ngày phát hành chính xác của Keylogger. Tuy nhiên cũng có nhiều người tin rằng nó được xuất hiện trong đầu những năm 90.

## Phân loại Keylogger

Keylogger được ghi nhận tồn tại dưới hai dạng: phần cứng và phần mềm.

### Keylogger phần cứng

Keylogger phần cứng xâm nhập vào máy thông qua con đường vật lý, nghĩa là phải có kẻ nào đó gắn nó vào phần cứng PC hoặc chèn nó vào cổng bàn phím giữa CPU và cáp bàn phím. Trong trường hợp này, nhiều kịch bản có thể xảy ra. Đầu tiên là do người thân xung quanh bạn chủ động cài đặt Keylogger vào máy tính. Những người này có thể là cha mẹ, người yêu, vợ/chồng hoặc ban quản lý tại cơ quan bạn làm việc cài đặt để giám sát hoạt động của bạn. Đấy là những đối tượng không có ý đồ xấu đối với bạn. Ngoài ra, còn có những kẻ xấu lợi dụng lúc bạn sơ hở, nhanh tay gắn nó vào máy tính của bạn để thu thập thông tin trái phép.

### Keylogger phần mềm

Keylogger phần mềm dễ lây nhiễm hơn, nên cũng phổ biến hơn. Con đường xâm nhập đầu tiên là thông qua mã độc. Như các phần mềm độc hại khác, bạn sẽ bị lừa nhấp vào các file/link đính kèm trong các chương trình thường xuyên được sử dụng như email, messenger, các mạng xã hội,…

Không những thế, các Trojan gây nhiễm Keylogger thường mang theo cả adware, spyware, ransomware hoặc một loại virus phổ biến khác. Ngoài kênh xâm nhập thông thường bằng mã độc, đa số trường hợp nhiễm Keylogger phần mềm còn lại cũng xuất phát từ những người thân xung quanh bạn – chúng tự lây nhiễm thông qua các gói phần mềm quản lý (parental controls) mà họ cài đặt vào thiết bị bạn sử dụng.

## Lợi ích và tác hại của Keylogger

### Lợi ích

* Giám sát năng suất làm việc của nhân viên: Để có thể giám sát năng suất làm việc của nhân viên từ xa, chắc chắn không có công cụ nào tốt hơn Keylogger.
* Duy trì việc kiểm tra con cái của bạn: Nếu các bạn biết con bạn đang tham gia vào loại hoạt động nào khi truy cập Internet, bạn sẽ dễ dàng hơn trong việc theo dõi thói quen của chúng. Bạn sẽ dễ dàng hơn nhiều để ngăn họ tham gia vào các hoạt động có hại trên Internet.
* Theo dõi các hoạt động của vợ/chồng: Nếu bạn thấy chồng/vợ mình có những hành động đáng nghi ngờ, không chung thủy. Các bạn có thể nhờ đến phần mềm này để nắm bắt được các hoạt động của họ trên internet.

### Tác hại

* Không giống như các phần mềm độc hại khác, xóa dữ liệu hoặc ăn cắp dữ liệu. Keylogger được thiết kế để không bị chú ý trong khi ghi lại thông tin của người dùng. Đó là lý do tại sao chúng rất khó bị phát hiện.
* Phần mềm thường được sử dụng cùng với các chương trình độc hại khác, nắm bắt các lần gõ phím và thông tin nhạy cảm (số tài khoản ngân hàng, mật khẩu, mã PIN,…) mà kẻ gian lợi dụng để đánh cắp dữ liệu bí mật của công ty, mạo danh người dùng hoặc thực hiện các giao dịch tài chính gian lận.

## Một số Keylogger phổ biến và ứng dụng phổ biến của Keylogger

### Một số Keylogger phổ biến

* Perfect Keylogger
* Easy Keylogger
* Active Keylogger

### Các ứng dụng phổ biến của Keylogger

#### Các ứng dụng tích cực

Nếu được sử dụng đúng mục đích tốt, nó có thể giúp các bậc phụ huynh giám sát hoạt động sử dụng máy tính của con cái mình. Hoặc các công ty có thể sử dụng keylogger để theo dõi hoạt động sử dụng máy tính trong giờ làm việc của nhân viên và việc này cần được sự đồng ý của các nhân viên. Keylogger cũng có thể được sử dụng để bảo vệ (ghi lại) mật khẩu và các dữ liệu khác trong trường hợp hệ điều hành gặp sự cố. Ngoài ra, gần đây các nhà khoa học đã bắt đầu sử dụng trình theo dõi thao tác bàn phím như một công cụ để nghiên cứu quá trình viết chữ của con người.

#### Các ứng dụng tiêu cực

Về mặt tiêu cực, keylogger thường được sử dụng cho các mục đích phạm pháp. Ví dụ: các Hacker sử dụng các chương trình phần mềm keylogger là để ghi lại mỗi và mọi thao tác bàn phím của máy tính mục tiêu để đánh cắp các thông tin nhạy cảm, private key, seed phase, số thẻ tín dụng, mật khẩu, email cá nhân, thông tin đăng nhập tài khoản ngân hàng…

# CHƯƠNG 2. CƠ SỞ LÝ THUYẾT CỦA KEYLOGGER

## Cách thức hoạt động của Keylogger

Cách hoạt động của keylogging

Giải thích về keylogging được ghép nối với bàn tay trên bàn phím máy tính đang được theo dõi bởi keylogger.

Các trình theo dõi thao tác gõ phím luôn có sẵn và có thể có một trình theo dõi được cài đặt trên chính thiết bị bạn đang sử dụng để đọc nội dung này. Bản thân phần mềm không nhất thiết có vấn đề nếu bạn đã ký thỏa thuận sử dụng thiết bị được cài đặt trên đó hoặc nếu nó được đóng gói trong bộ phần mềm của thiết bị của bạn. Điều khiến các công cụ này trở nên có vấn đề là các vấn đề về ý định của tác nhân và sự đồng ý của nạn nhân.

Cho dù việc sử dụng là hợp pháp hay bất hợp pháp, tất cả các cơ chế keylog về cơ bản hoạt động theo cùng một cách. Chúng ghi lại mọi tương tác bàn phím mà người dùng có, cho phép bên thứ ba xem nhật ký hoàn chỉnh của mọi email, tin nhắn tức thì, truy vấn tìm kiếm, mật khẩu, tên người dùng hoặc các chuỗi có khóa khác mà người dùng nhập. Phần mềm độc hại cho phím bấm có nhiều dạng:

Email lừa đảo: Bằng cách nhấp vào liên kết hoặc tải xuống tệp đính kèm trong email lừa đảo, tin nhắn văn bản, tin nhắn tức thì hoặc bài đăng trên mạng xã hội, bạn có thể vô tình tải xuống phần mềm độc hại được thiết kế để theo dõi các lần gõ phím.

Virus Trojan: Được đặt theo tên con ngựa gỗ khổng lồ mà Hy Lạp từng xâm nhập thành Troy trong Chiến tranh Troy, tin tặc lừa người dùng tải xuống virus Trojan bằng cách ngụy trang nó thành một tệp hoặc ứng dụng hợp pháp.

Khai thác zero-day: Khai thác zero-day xảy ra khi tin tặc phát hiện ra các lỗ hổng bảo mật tiềm ẩn của phần mềm và sử dụng chúng để phân phối phần mềm độc hại thông qua các chiến thuật như tập lệnh trang web độc hại và Trojan. Các nhà phát triển biết về các lỗ hổng bảo mật quá muộn để bảo vệ người dùng. Những điều này đặc biệt nguy hiểm vì một khi hệ thống bị nhiễm, chúng sẽ trở nên dễ bị tấn công hơn.

Hệ thống bị nhiễm: Keylogger có thể lợi dụng thiết bị hoặc hệ thống đã bị nhiễm và cài đặt phần mềm độc hại khác vào hệ thống đó.

Phần mềm độc hại keylogging có thể lây nhiễm vào máy tính của bạn thông qua nhiều cơ chế giống như các loại vi rút thông thường khác, nhưng nó cũng có thể được mua và tải xuống có chủ ý. Nói tóm lại, keylogger có thể là công cụ hoặc vũ khí, tùy thuộc vào người đang cài đặt chúng và cách họ sử dụng thông tin có được.

## Keylogger được sử dụng để làm gì và có thể thu thập những gì

### Keylogger được sử dụng để làm gì

Ba cách sử dụng keylogger hợp pháp và bất hợp pháp phổ biến xuất hiện cạnh nhau trong hai cột.

#### Ví dụ về keylog hợp pháp

Việc sử dụng hợp pháp keylogger phụ thuộc vào sự đồng ý của người dùng (tùy thuộc vào luật pháp địa phương), liệu chúng có được sử dụng với mục đích xấu để lấy cắp thông tin cá nhân hay không, ai sở hữu thiết bị mà chúng được cài đặt và việc sử dụng có làm nạn nhân của ai đó theo cách phá vỡ bất kỳ cách nào khác hay không luật áp dụng. Dưới đây là một số ví dụ về keylog hợp pháp tiềm năng:

* Giám sát dữ liệu trải nghiệm người dùng
* Kiểm soát của phụ huynh để giám sát và bảo vệ hoạt động trực tuyến của trẻ em
* Ghi lại việc sử dụng trên thiết bị cá nhân do người dùng keylogger sở hữu
* Khắc phục sự cố mạng, phần mềm hoặc phần cứng
* Trao đổi dữ liệu công ty và giám sát truy vấn tìm kiếm
* Giám sát tận dụng việc sử dụng bởi một công ty hoặc tổ chức công, chẳng hạn như thư viện
* Mọi hoạt động sử dụng hợp pháp được đồng ý thông qua hợp đồng hoặc thỏa thuận người dùng
* Về cơ bản, việc sử dụng hợp pháp tuân theo luật pháp địa phương, sự đồng ý của người dùng và không có ý định sử dụng sai thông tin của người dùng.

#### Ví dụ về keylog bất hợp pháp

Keylogging bất hợp pháp trở nên phức tạp vì đôi khi việc sử dụng hợp pháp tiềm ẩn có thể phân ranh giới giữa phi đạo đức và bất hợp pháp. Nói chung, việc sử dụng trở nên bất hợp pháp chủ yếu khi dẫn đến dữ liệu bí mật bị đánh cắp hoặc khi phần mềm / phần cứng được cài đặt trên thiết bị do người khác sở hữu, như được nêu dưới đây:

* Trộm cắp thông tin tài khoản
* Thu thập thông tin nhạy cảm
* Giám sát khi sự đồng ý bị từ chối một cách rõ ràng thông qua một liên hệ ràng buộc pháp lý
* Thông tin thẻ tín dụng và thu thập mã PIN
* Cài đặt phần mềm hoặc phần cứng trên thiết bị của người khác

### Keylogger có thể thu thập những gì

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,…

Như bạn thấy, 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).

## Cách phòng tránh và phát hiện và xử lý khi bị dính Keylogger

### Cách phòng tránh

Keylogger thường cài đặt vào máy qua hai con đường chính: được cài đặt hoặc bị cài đặt.

#### Phòng ngừa "được cài đặt”

Phương pháp sau chỉ có tác dụng với chủ máy (người nắm quyền root hoặc administrator). Cách tốt nhất là không cho ai sử dụng chung máy tính. Bảo mật máy bằng cách khóa lại bằng các chương trình bảo vệ, hoặc mật khẩu khi đi đâu đó. Nếu phải dùng chung nên thiết lập quyền của người dùng chung đó thật thấp (guest đối với Windows XP, user đối với Linux) để kiểm soát việc cài đặt chương trình của họ.

#### Phòng ngừa "bị cài đặt”

Bị cài đặt là cách đê nói đến các trường hợp Keylogger vào máy không do người nào đó trực tiếp đưa vào trên máy đó mà do Trojan, Virus, Spyware cài đặt vào máy nạn nhân mà nạn nhân không hè hay biết. Các biện pháp phòng ngừa:

* Không tùy tiện mở các tập tin lạ, không rõ nguồn góc (đặc biệt chú ý các tập tin có đuôi \*.exe, \*.com, \*.bat, \*.scr, \*.swf, \*.zip, \*.rar, \*.js, \*,gif...). Tốt nhât là nên xóa đi, hoặc kiểm tra (scan) bằng một chương trình antivirus và một chương trình antispyware, vì nhiêu chương trình antivirus chỉ có thê tìm thây virus, không thê nhận biệt spyware.
* Không vào các trang web lạ, đặc biệt là web "tươi mát" vì có thể các trang web này ân chứa một loại worm, virus, hoặc là mã độc nảo đó có thê âm thâm cài đặt.
* Không click vào các đường link lạ do ai đó gửi cho chúng ta.
* Không cài đặt các chương trình lạ (vì nó có thê chứa virus, trojan).
* Không download chương trình từ các nguồn không tin cậy. Nếu có thể xem xét chữ ký điện tử, đê chắc chắn chương trình không bị sửa đôi.
* Hạn chế download và sử dụng cracked-program.
* Luôn luôn tự bảo vệ mình bằng các chương trình chuyên dùng chống virus, chông spyware (antivirus, antispyware) và dựng tường lửa (firewall) khi ở trong Internet.
* Thường xuyên cập nhật đầy đủ các bản cập nhật bảo mật của hệ điều hành.
* Hoặc chúng ta có thê download một số phần mềm chống Keylogger về đề bảo vệ

### Cách phát hiện Keylogger

Phát hiện keylogger không khó với một người có hiểu biết chút về máy tính, nhưng cũng khá rắc rối với một người bình thường. Sau đây là một số cách phát hiện keylogger:

1. Sử dụng phần mềm StartUp Control để tìm xem có file lạ nào nạp khởi động cùng Windows hay không.

2. Có khi nó gắn nó vào một process khác mình không nhìn được, nhưng vẫn lộ ra ở danh sách các process đang chạy trên máy. Bấm phím Ctril + Alt + Delete (Windows Task Manager) và tìm trong TAB Processes xem có process nào lạ không. Khuyến khích dùng Process Explorer hơn.

Nhưng nếu như bạn không phải là người thành thạo máy tính thì, không biết chính xác là máy tính này có keylogger hay không thì có thể sử dụng thủ thuật sau đây để lừa lại chính tên kẻ cắp.

### Cách xử lý khi bị dính Keylogger

Cài đặt một chương trình diệt virus tốt sẽ có thể giúp bạn được an toàn và tránh việc bị các malware cài đặt các phần mềm Keylogger vào máy tính.

Nếu bạn không muốn cài đặt các chương trình diệt Virus vì một số lý do nào đó thì một lựa chọn khác cho bạn lài đặt một chương trình chống Keylogger, vì các chương trình này được thiết kế đặc biệt để phát hiện, gỡ bỏ và phòng ngừa các cuộc tấn công Keylogger.

Luôn cẩn thận với các tệp đính kèm và đường dẫn trong email và không nên bấm vào các quảng cáo và các trang web không rõ nguồn gốc.

Các bạn nên cập nhật thường xuyên các ứng dụng phần mềm và hệ điều hành của bạn. Nếu phát hiện sự xuất hiện của các tập tin chạy dưới User name không phải là System, hãy tìm hiểu kỹ xem nó có liên quan đến hệ thống hay không, bạn nên tìm kiếm trên mạng và cố gắng xác định liệu đó là từ một chương trình hợp pháp hay từ một keylogger.

Khi đã phát hiện máy tính có phần mềm keylogger lạ đang chạy, bạn có thể tiến hành gỡ cài đặt và xóa nó. Trong trường hợp bạn đã xóa và gỡ cài đặt phần mềm keylogger mà vẫn thấy máy tính mình hoạt động một cách bất thường thì các bạn có thể nghĩ tới việc cài lại Windows.

## Ví dụ về một số cách để tìm và xóa Keylogger trên một số Keylogger phổ biến

### Easy Keylogger

Sau khi cài đặt xong và khởi động Easy Keylogger có 1 biểu tượng chạy ở system tray.

Chức năng chính của Easy Keylogger :

* Cho phép đặt phím tắt, mặc định : Shift + Ctrl + alt +V
* Tập tin dùng để Capture thao tác : Ekey.dll
* Chỉ có thê Capture thao tác, không có chế độ chạy ẳn, không có chức năng đính kèm Keylogger

\* Ghi chú nhỏ : Có thẻ máy tính của chúng ta đang chạy rất nhiều chương trình ứng dụng, nên khi dùng lệnh : tasklist /m

Chúng ta sẽ khó theo dõi được, để đạt hiệu quả cao chúng ta hãy xuất vào I tập tin tạm (stout) ra Ï tập tin .txt

Dùng lệnh :

1. Vào mục Start -> Run gõ : cmd

2. Ở màn hình Dos gõ : tasklist /m > ctemp.txt

(Ở đây chúng ta ví dụ xuất vào ô đĩa C với tập tỉn temp.txÐ)

#### Cách tìm

Yêu cầu : Chỉ áp dụng được với Windows 2K và XP (Windows 9x không hỗ trợ)

1. Vào mục Start -> Run gõ : cmd

2. Ở màn hình Dos gõ : tasklist /m Ekey.dll

Nếu không có Keylogger bạn sẽ nhận được 1 thông báo lỗi :

INEO: Không tasks running with the specified criteria.

Nếu có Keylogger màn hình sẽ hiên thị :

Image Name PID Modules Diễn giải

TOTALCMD\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* ..... 2040 ----- ekey.dll <--- quen thuộc

Easy Keylogger\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*..... 2340 ----- ekey.dll <--- Keylogger

Sở dĩ chúng ta tìm tập tin Ekey.dll là vì đây chính là tập tin Easy Keylogger dùng để ghỉ lại thao tác trên máy tính.

#### Cách diệt : (Lưu ý ở đây sẽ có nhiều cách diệt khỏi Process)

Đã tìm được tên đích danh rồi chúng ta hãy thực hiện các bước sau để tiêu diệt :

1. Cách diệt thông thường :

+ Vào mục Start -> Run gõ : emd

+ Ở màn hình Dos gõ : taskkill /f /im Easy Keylogger\*\*\*\*\*\*\*\*\*\*\*\* /

ERROR: Invalid ArgumenưOption - 'Key'.

2. Cách diệt sử dụng wildcard :

+ IProgram Eiles>taskkill /f /im EasyKe~ | \*\* \*\*\*\*\*\*\*\*\*\*\*\*\* /t

ERROR: The process "EasyKe~ | \*\*\*\*\*\*\*\*\*\*\*\*\*\*" not found.

3. Cách diệt sử dụng được :

+ Vào mục Start -> Run gõ : cmd

+ Ở màn hình Dos gõ : taskkill /f /fï "pid ge 2340" /im \*

Giải thích : Để hiểu được chúng ta hãy xem lại phía trên khi chúng ta tìm Ekey.dll

'Windows đã phát hiện ra được răng Easy Keylogger đang chạy ở thread 2340 đúng không . Đây là cách dùng đê loại bỏ tên tập tin dài.

4. Tắt tất cả các chương trình đang chạy hiện thời.

5. Mở Explorer tìm và xóa các tập tin Easy Keylogger\*\*\*\*\*\*\*\*\*\*\*\*Ekey.dll

### Perfect Keylogger

#### Cách tìm

Yêu cầu : Chỉ áp dụng được với Windows 2K và XP (Windows 9x không hỗ trợ)

1. Vào mục Start -> Run gõ : cmd

2. Ở màn hình Dos gõ : tasklist /m bpkhk.dll

Nếu không có Keylogger chúng ta sẽ nhận được 1 thông báo lỗi :

Info: Không tasks running with the specified criteria.

Nếu có Keylogger màn hình sẽ thị:

Image Name PID Modules diễn giải

Explorer 468 bpkhk.dll<--- quen thuộc

DUMeter 1444 bpkhk.dll<--- quen thuộc

ctfmon 1548 bpkhk.dll<--- quen thuộc

acrotray 1820 bpkhk.dll<--- quen thuộc

notepad 1956 bpkhk.dll<--- quen thuộc

firefox 2012 bpkhk-dll<--- quen thuộc

bdmcon 1744 bpkhk.dll<--- quen thuộc

TOTALCMD 2396 bpkhk-dll<--- quen thuộc

bpk 2812 bpkhk-dll<--- Keylogger

Sở dĩ chúng ta tìm tập tin bpkhk.dil là vì đây chính là tập tin Perfeet Keylogger

dùng để ghi lại thao tác trên máy tính.

#### Cách diệt

Đã tìm ra đích danh chúng ta hãy thực hiện các bước sau để tiêu diệt nó:

1, Vào mục Start -> Run gõ : cmd.

2. Ở màn hình Dos gõ : taskkill/f /ñm bpk/L

3. Tắt tất cả các chương trình đang chạy hiện thời (Explorer, bdswitch, DUMeter )

4. Mỡ Explorer vào thư mục Windows\System32 xóa các tập tin bpk, bpkhk.dll,

bpkwb.dll

### Active Keylogger

#### Cách tìm

Sau khi cải đặt xong và khởi động Active Key Logger có 1 biểu tượng chạy ở system tray.

Chức năng bên trong của Active Keylogger

- Tập tin dùng để Capture : smode.dIl, CMD16.dIL

- Chức năng Security : (cho phép ân hoàn toàn trên hệ thống)

+ Disable Task Manager

+ Remove Shortcut from Desktop

+ Remove Shortcut from Start Thực đơn

+ Remove Active Keylogger from Uninstall List

- Stealth Mode : Cho phép chạy ân

Phân tích sơ bộ về Active Keylogger

- Có khả năng Capture tắt cả các thao tác trên máy tính.

- Không có khả năng tự đính kèm, tuy nhiên vẫn có thể dùng một số chương trình khác đề đính kèm vào được

- Cho phép gởi tập tin log qua email (mặc định port 25). tập tỉn log có tên \*.kl (có thể thay đổi được)

#### Cách diệt

Chúng ta hãy dùng cách tìm và diệt giống như của Easy Keylogger, vì Active KeyLogger cũng là I tập tỉn có tên dài quá 8 ký tự.

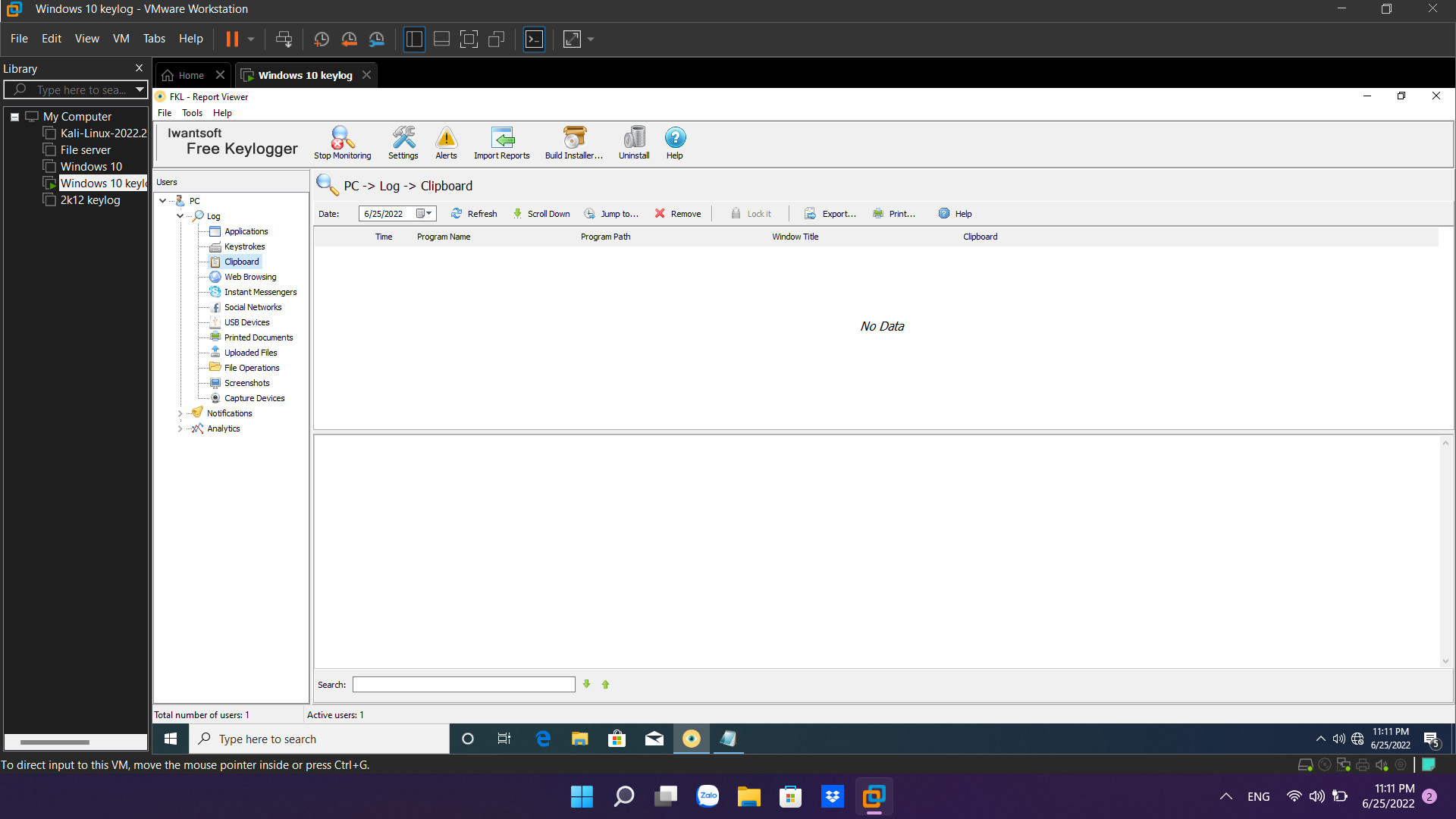
# CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM

## Yêu cầu chuẩn bị

* Máy windown 10
* Phần mềm Free Keylogger

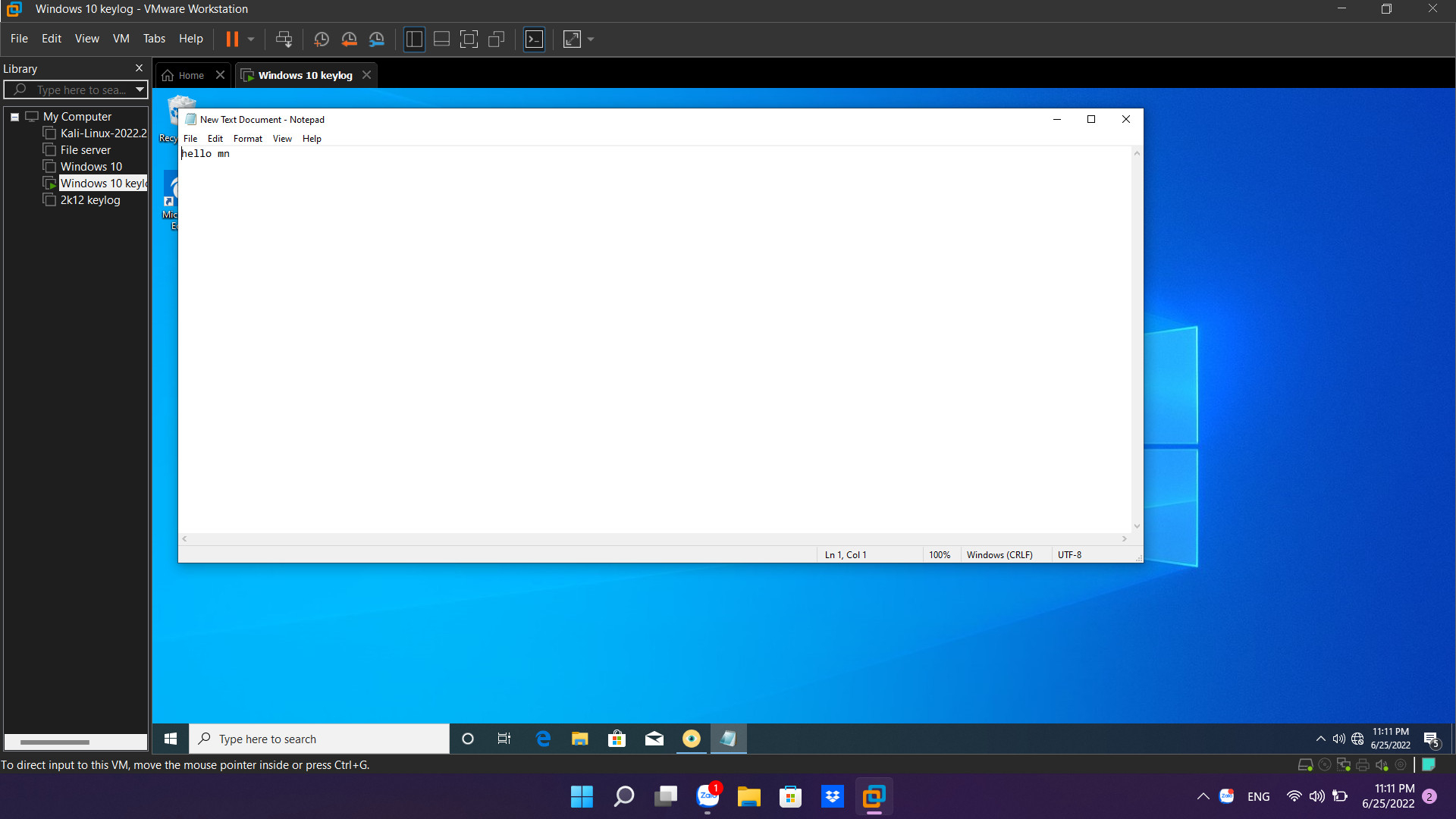
## Ghi lại file của Keylogger

Bước 1: Cài đặt Keylogger vào win 10



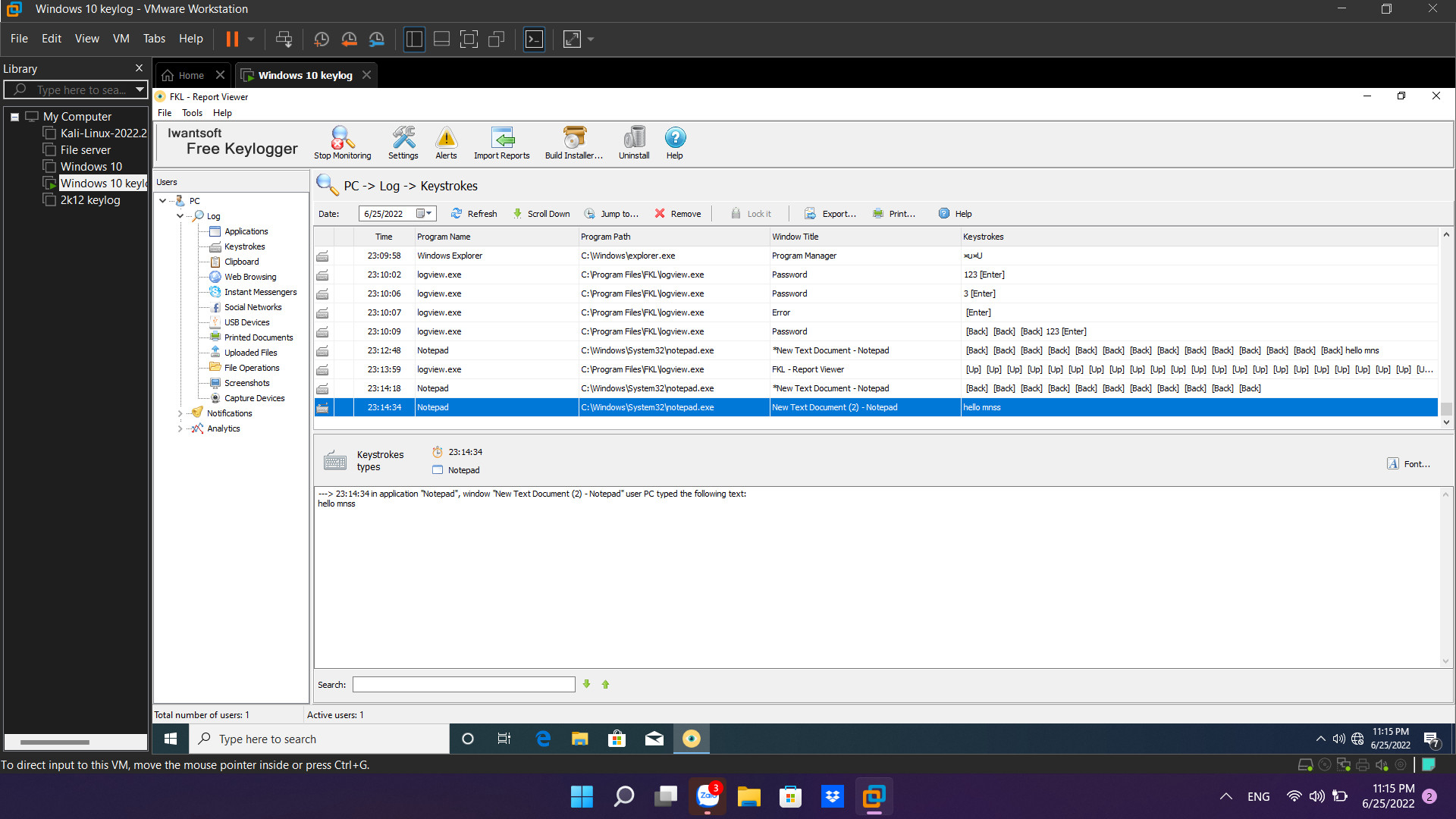
Hình 3.2.1 Giao diện của Keylogger

Bước 2: Chúng ta tắt hoạt động của keylogger, kiểm tra Task Manager để đảm bảo Keylogger đã ẩn hoạt động hoàn toàn. Sau đó chúng ta sẽ tiến hành tạo ra 1 file text và nhập nội dung vào



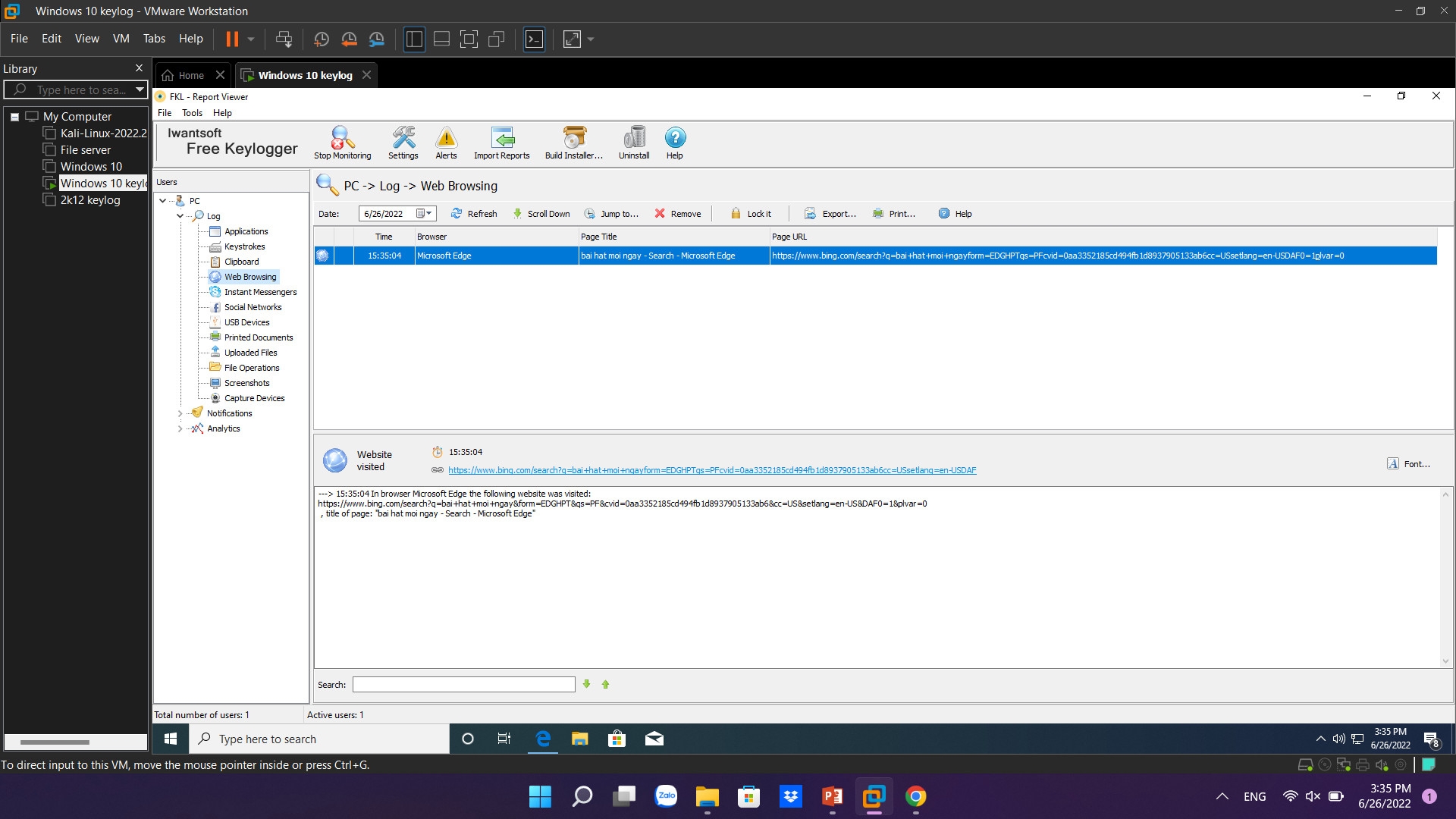
Hình 3.2.2 Tạo file text

Bước 3: Hệ thống sẽ ghi nhận file text đã nhập



Hình 3.2.3 Hệ thống ghi nhận file text

Ngoài ra thì Keylogger cũng có thể ghi lại các hoạt động khác như lịch sử Website đã truy cập của máy nạn nhân



Hình 3.2.4 Hệ thống ghi nhận lịch sử truy cập Website

# KẾT LUẬN

Qua quãng thời gian làm đề tài này em đã có thêm thật nhiều kiến thức mới mẻ và thú vị . Cùng với những kiến thức cơ bản về HĐH windows song song với quá trình tìm hiểu về Keylogger, để dựa vào những kiến thức nền tảng và đầy tính chất mang tính thực tiễn em viết một chương trình Keylogger đơn giản với mục đích giám sát.

Kết quả đạt được: Do thời gian thực trong một khoảng thời gian ngắn và em chưa có hiểu biết sâu về hệ điều hành windows cùng một số thư viện cũng như các hàm cần thiết. Em đã viết được một chương trình Keylogger ghi nhận file text.

Tương lai phát triển : Trong tương lai em sẽ có gắng hoàn thiện thêm một số chức năng nữa cho Keylogger, để Keylogger này tuy chỉ dùng với mục đích giám sát nhưng sẽ hiệu quả và mang tính chất thực tiễn tốt hơn. Trong quá trình thực hiện đề tài, dù đã rất có gắng, nhưng do trình độ, kiến thức, thời gian còn nhiều hạn ché, không thể tránh khỏi những thiếu sót trong lúc thực hiện. Em rất mong được sử đóng góp ý kiến, sửa chữa, và định hướng phát triển đề tài được hoàn thiện hơn. Rắt cám ơn thầy cô đã dành thời gian để đọc và đánh giá đề tài.

# TÀI LIỆU THAM KHẢO

[1] <https://websitehcm.com/keylogger-la-gi-tim-hieu-ve-keylogger/>

[2] <https://www.slideshare.net/vumanhson98/tm-hiu-keylogger-v-thit-k-chng-t...eylogger>