# PHÁT HIỆN, PHÒNG CHỐNG PHẦN MỀM GIÁN ĐIỆP KEYLOGGER

**Nguyễn Đăng Tiến***
*Trường Đại học Kỹ thuật – Hậu cần Công an Nhân dân*

TÓM TẮT

Phần mềm gián điệp là một trong những yếu tố góp phần gây mất an ninh mạng Việc phát hiện loại bỏ những phần mềm loại này là một trong những nhu cầu cấp thiết hiện nay Trong bài báo này chúng tôi trình bày quá trình xây dựng một phần mềm gián điệp Keylogger, triển khai thử nghiệm trên môi trường thực tế và sử dụng một số công cụ để quan sát hoạt động. Các kết quả thực nghiệm cho thấy phần mềm xây dựng được có khả năng thu thập được thông tin nhập từ bàn phím từ máy tính bị theo dõi và chuyển về cho chủ thể theo dõi Dựa trên các dấu hiệu hoạt động, chúng tôi tổng kết các dấu hiệu phát hiện, loại bỏ phần mềm này Các kỹ thuật này sẽ góp phần tích cực vào việc bảo vệ dữ liệu người sử dụng, có ý nghĩa quan trọng trong thực tế khi có thể là nền tảng để xây dựng các công cụ phát hiện và loại trừ phần mềm gián điệp

**Từ khóa:** *An toàn thông tin, Phần mềm gián điệp Keylogger, Wireshark, File nhận ký, Lưu lượng mạng*

## MỞ ĐẦU

Mạng Internet là kênh thông tin có sức lan tỏa nhanh chóng và mạnh mẽ, giúp người sử dụng bổ sung tin tức đa lĩnh vực, cập nhật kiến thức mới với tốc độ nhanh chóng và chi phí thấp. Sự bùng nổ của công nghệ mang xã hội đã đẩy mạnh quá trình liên kết nhiều người, nhóm người với nhau, có các cơ chế cập nhật và quảng bá tin tức hiệu quả, cung cấp một lượng thông tin lớn tới người sử dụng. Hiện nay nước ta đang phát triển mạnh mẽ về kinh tế, văn hóa, xã hội và công nghệ thông tin có phần đóng góp không nhỏ trong sự phát triển đó Tuy nhiên, đi kèm với sự phát triển của công nghệ mạng là các nguy cơ mất an toàn của các hệ thống thông tin [3], [4], [5], [8], [10]. Việc mất hoặc lộ lọt thông tin luôn là chủ đề nhận được sự quan tâm rộng rãi từ cộng đồng nghiên cứu cũng như các đơn vị ứng dụng. Các kỹ thuật tấn công phá hoại hệ thống thông tin là một trong những vấn đề nóng và có tác động trực tiếp tới các tổ chức, cá nhân tham gia sử dụng mạng [6], [7], [9], [11]. Với lý do đó, bảo vệ hệ thống thông tin khỏi các cuộc tấn công, phá hoại là một trong những vấn đề cấp bách hàng đầu hiện nay. Trong số các loại mã độc, phần mềm gián điệp Keylogger [1], [2] là công cụ thường được sử dụng do tính đơn giản và hiệu quả cao. Một phần mềm Keylogger có khả năng bí mật ghi lại các thao tác gõ phim, chứa tên đăng nhập, mật khẩu, của các tài khoản mang xã hội, tài khoản ngân hàng, thông tin bí mật sau đó truyền qua mạng máy tính để gửi về cho chủ sở hữu [10], [16], [17]. Để bảo vệ an toàn thông tin người sử dụng trên máy tính cá nhân, cần hiểu được cơ chế làm việc và các đặc điểm hoạt động của phần mềm Keylogger từ đó có các biện pháp hiệu quả để phát hiện và loại bỏ. Trong bài báo này, chúng tôi xây dựng một phần mềm gián điệp theo dõi hoạt động của bàn phím để làm rõ một số cơ chế phát hiện và phòng chống phần mềm gián điệp, trên cơ sở đó đề xuất một số biện pháp hiệu quả để phát hiện và loại trừ Keylogger. Chúng tôi xây dựng một chương trình Keylogger với mục tiêu để kiểm chứng nguyên lý hoạt động của một phần mềm theo dõi bàn phím trong thực tế, tìm ra các đặc điểm hoạt động của loại phần mềm này, trên cơ sở đó rút ra các cách thức để phát hiện và ngăn chặn Keylogger. Phần 2 trình bày quá trình xây dựng một phần mềm cùng các kịch bản thử nghiệm. Phần 3 nêu một số đặc điểm để phát hiện và loại bỏ Keylogger và đưa ra một số đề xuất để phát triển trong tương lai.

## XÂY DỰNG VÀ THỬ NGHIỆM KEYLOGGER

### Tình hình nghiên cứu trong và ngoài nước

Các công cụ phần mềm gián điệp được ưa dùng do sự đơn giản và hiệu quả cao. Theo thông tin do Wikileaks tiết lộ trong tháng 2 năm 2017 về hoạt động của Cục Tình báo trung ương Hoa Kỳ cho thấy, CIA sử dụng rất nhiều loại phần mềm gián điệp khác nhau để

* *Email: dangtient36@gmail.com*

theo dõi máy tính. Sản phẩm Keylogger cũng hiện diện trong danh sách các phần mềm CIA sử dụng. Báo cáo cho thấy, các công cụ Keylogger đều được xây dựng và cài đặt theo nguyên tắc chung mà chúng tôi sẽ trình bày trong bài báo này. Nhưng cùng với sự phát triển của công nghệ, các phần mềm này được thiết kế để nâng cao khả năng vượt qua được các phần mềm diệt Virus hiện nay, nhằm tăng hiệu quả hoạt động của phần mềm, lấy được nhiều dữ liệu về chủ thể bị theo dõi nhưng vẫn đảm bảo khả năng không bị phát hiện [12], [16], [18]. Các nghiên cứu hiện nay về lĩnh vực này đều tập trung vào các kỹ thuật để né tránh các phần mềm diệt Virus. Với các nghiên cứu ở nước ta, chúng tôi chưa thấy có một bài báo nào mô tả chi tiết các kỹ thuật trong lĩnh vực này. Vì vậy, bài báo của chúng tôi sẽ góp phần vào việc làm rõ một số vấn đề liên quan đến chủ đề cũng như đưa ra biện pháp tăng cường khả năng tìm và diệt phần mềm gián điệp theo dõi bàn phím.

**Nguyên lý hoạt động của KeyLogger**

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 nhắn thông qua ứng dụng lập trình socket [1], [2].

*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.

Hoạt động của một Keylogger được minh họa ở đoạn giả mã nguồn (pseudo-code) sau đây:

```
FtpConnection ftp = new
FtpConnection();
while (1) do {
  call(hook);
  data = getKeyboarData();
  f = saveToFile(data);
  ftp.send(f);
  sleep(t);
}
```

Kết nối FTP được tạo lập để truyền dữ liệu ra ngoài. Hàm hook được thực thi để gọi ngắt bàn phím, thu thập dữ liệu gõ phím và ghi thành file trên đĩa cứng. Hàm sleep(t) để ngưng hoạt động trong một thời gian nhất định, việc gửi dữ liệu được thực hiện theo định kỳ để tránh bị phát hiện. Tham số t có thể được điều chỉnh dựa theo yêu cầu của người điều khiển phần mềm Keylogger.

Keylogger theo dõi các thông điệp mà người dùng giao tiếp với hệ điều hành, lưu trữ ở các tập tin với đường dẫn xác định. Để tránh bị phát hiện, các đường dẫn, tập tin này có một số đặc điểm như sau:

- Có vị trí mà người dùng thường ít khi truy cập tới hoặc trong các chương trình bình thường để tránh bị nghi ngờ.
- Có các thuộc tính: Hidden, Read only, System.
- Phần mở rộng file là, hoặc không có phần mở rộng.
- Được mã hóa phức tạp.

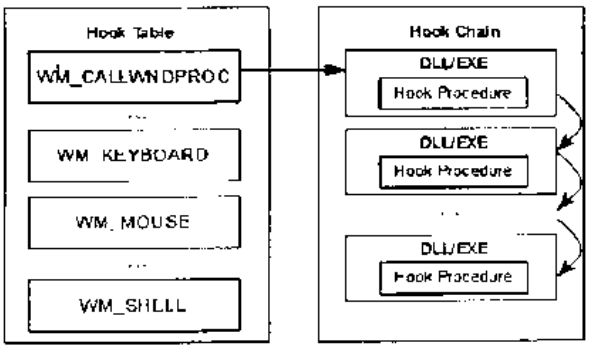
Các phương thức để Keylogger gửi các tập tin log, ra ngoài có thể là các dịch vụ có sẵn như thư điện tử, dịch vụ truyền file FTP hoặc truyền nhận dữ liệu qua giao thức TCP/IP bằng lập trình Socket.

*Kỹ thuật hook trong Windows*

Windows là một hệ điều hành đa nhiệm, cho phép nhiều ứng dụng cùng thực thi trên máy

trong cùng một thời điểm. Để quản lý quá trình tương tác với từng đối tượng, Windows sử dụng sự kiện (event) là hành động tác động với từng đối tượng trong một thời điểm cụ thể. Khi một sự kiện xảy ra, hệ điều hành Windows gửi một thông điệp đến đối tượng. Các sự kiện thường diễn ra trên Windows là kích chuột (click, double click), các sự kiện bàn phím (nhấn phím, nhả phím) và các sự kiện với từng cửa sổ chương trình (Activate, Load, Unload). Trong Windows, hook là khái niệm để chỉ việc người lập trình hệ thống chăn bắt các sự kiện trước khi được gửi đến đối tượng. Hàm cho phép thực hiện chức năng này được gọi là hàm lọc (filter) hay các thủ tục hook (hook function) Windows có danh sách các hàm lọc cho từng loại thủ tục và được gọi là chuỗi (hook chain).

Hệ điều hành tìm trong hook chain các hàm lọc tương ứng với một sự kiện khi nó xảy ra. Sau khi một hàm lọc thực hiện xong, sẽ chuyển quyền điều khiển cho hàm lọc kế tiếp trong danh sách và khi hàm lọc cuối cùng được thực hiện thì quyền điều khiển được trả về cho hệ thống. Hình 2 minh họa kiến trúc hook trong Windows.




Hình 1. *Kiến trúc Hook trong Windows* [1], [2]

WH_CALLWNDPROC: Cài đặt một thủ tục hook để giám sát các thông điệp trước khi hệ thống gửi chúng đến cửa sổ đích. Loại hook này chỉ cho phép kiểm tra các thông điệp mà không thể chỉnh sửa thông điệp đó; sau khi bị thủ tục hook kiểm tra, thông điệp tiếp tục được truyền đến cửa sổ đích.

WH_KEYBOARD: Thủ tục hook bắt các sự kiện nhận được từ bàn phím như nhấn phím, nhả phím. Loại hook này có thể được gọi trong phạm vi luồng (thread) đã cài đặt nó, việc gọi này được thực hiện bằng cách gửi một thông điệp đến các luồng đã cài đặt hook. Vì vậy, các luồng đã cài đặt hook phải có một vòng lặp thông điệp

WH_KEYBOARD_LL: Cài đặt một thủ tục hook ở mức thấp để theo dõi các sự kiện nhập vào từ bàn phím. Các luồng đã cài đặt hook phải có một vòng lặp thông điệp. Bàn phím nhập vào có thể đến từ trình điều khiển bàn phím cục bộ hoặc từ việc gọi các hàm sự kiện bàn phím.

Tùy theo các sự kiện mà quá trình hook được phân loại thành kiểu khác nhau. Có hai loại ngắt chính là: Hook cục bộ (thread hook) và hook toàn cục (global hook). Các Hook toàn cục có ảnh hưởng trên cả hệ thống thì hook cục bộ chỉ có ảnh hưởng với một cửa sổ hiện hành Ngoài ra, để sử dụng được hook toàn cục thì hàm lọc phải nằm trong một thư viện liên kết động (Dynamic link library/ DLL)

Các giao diện lập trình ứng dụng (API) của Windows thường được cung cấp dưới dạng các thư viện liên kết động. Thư viện liên kết động là nền tảng của hệ điều hành Windows kể từ các phiên bản đầu tiên. Khác với thư viện tĩnh được liên kết trong quá trình biên dịch chương trình trước khi chạy, thư viện liên kết động được chương trình liên kết ngay trong thời gian chạy. Các ứng dụng Windows thường có liên kết với ba thư viện liên kết động quan trọng.

- Kernel32.dll cài đặt các hàm để quản lý tiến trình, bộ nhớ và luồng,
- User32.dll cài đặt các hàm thực hiện các nhiệm vụ giao diện người dùng như tạo cửa sổ, gửi thông điệp;
- GDI32.dll có cài đặt các hàm về đồ hoạ và hiển thị ký tự.

Tập tin DLL có chứa cả mã máy, dữ liệu (data) và các tài nguyên (resources). Định dạng của tập tin thư viện liên kết động DLL cũng giống định dạng của tập tin thực thi, đều có cấu trúc PE (Portable Executable) trong Windows 32-bit và 64-bit hoặc New Executable trong Windows 16-bit

Windows API là các thư viện được xây dựng sẵn để hệ điều hành Windows quản lý, trao đổi với phần cứng và thiết bị ngoại vi, các hàm Windows API này được viết và đóng gói

trong các file thư viện liên kết động nằm trong thư mục hệ thống của Windows Các chương trình ứng dụng của Windows sử dụng các hàm trong DLL dưới dạng mã máy mà không cần biết tới các thiết kế bên trong của các thư viện này. Chương trình sẽ gọi các hàm này trong thư viện liên kết động thay vì tất cả các chương trình phải viết lại mã của một hàm mỗi khi muốn sử dụng. Kỹ thuật này tăng cường tái sử dụng (re-use) và giúp tiết kiệm công sức và chi phí mỗi khi xây dựng một chương trình ứng dụng trên Windows.

Các thư viện liên kết động thường không thực thi trực tiếp và không nhận các dữ liệu nhập của người dùng thông qua vòng lặp thông điệp như các chương trình thực thi. Đây chỉ là các tập tin DLL tách riêng thực hiện các nhiệm vụ khác nhau và chỉ được đưa vào hoạt động khi các chương trình gọi một trong các hàm có trong thư viện DLL đó hoặc quyết định tải chúng

Việc sử dụng thư viện liên kết động DLL có những ưu điểm sau:

- Giảm không gian sử dụng của bộ nhớ;
- Có thể đóng gói và đưa vào chương trình khác;
- Tạo ra khả năng tương tác giữa các ngôn ngữ lập trình khác nhau;
- Dễ dàng hỗ trợ sau khi đã chuyển giao ứng dụng cho khách hàng.

Hàm SetWindowsHook cài một hàm lọc vào hook chain trong hệ điều hành Windows như minh họa ở đoạn mã nguồn sau.

```
HHOOK WINAPI SetWindowsHookEx(
  _In_ int       idHook,
  _In_ HOOKPROC  lpfn,
  _In_ HINSTANCE hMod,
  _In_ DWORD     dwThreadId
);
```

Hàm CallNextHookEx chuyển thông tin ngắt đến hàm lọc tiếp theo danh sách hook chain (Hình 3).

```
LRESULT WINAPI CallNextHookEx(
  _In_opt_ HHOOK  hhk,
  _In_     int    nCode,
  _In_     WPARAM wParam,
  _In_     LPARAM lParam
);
```

Hàm bắt phím từ thao tác của người sử dụng

```
LRESULT CKeyexeDlg::processkey(WPARAM w, LPARAM l){
     GetKeyNameText(l,buffer,20);
     _strlwr(buffer);
     if(strlen(buffer)>1){
        subst("shift","<SHIFT>");
        subst("right shift","<SHIFT>");
        subst("tab","<TAB>");
        subst("space"," ");
        subst("backspace","<BACKSPACE>");
        subst("delete","<DEL>");
        subst("left","<LEFT>");
        subst("down","<DOWN>");
        subst("up","<UP>");
        subst("right","<RIGHT>");
        subst("num /","/");
        subst("num *","*");
        subst("num -"," ");
     //các phím số
        subst("num 0","0");
        subst("num 1","1");
        subst("num 2","2");
        ...
     //các phím điều khiển
        subst("num enter","<ENTER>");
        subst("num del","<DEL>");
        subst("esc","<ESC>");
```

```
        subst("enter","<ENTER>");
        subst("caps lock","<CAPSLOCK>");
        ...
    //ghi dữ liệu ra ổ cứng
    diskfile->Write(buffer,strlen(buffer));
    if(keycount>50)
    {
        diskfile->Flush();
        keycount = 0;
    }
```

Tất cả các phím điều khiển sẽ được lưu lại ở dạng text rõ để người nhận dữ liệu có thể đọc được các ký tự nhập vào.

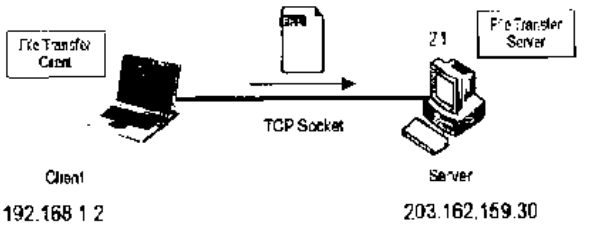
Khi gọi hàm processkey(), tất cả các thao tác gõ phím sẽ được chuyển thành ký tự tương ứng, cả các ký tự điều khiển như xóa (delete), shift, control Tất cả dữ liệu được lưu vào trong file trên ổ cứng. Các hook hệ thống đòi hỏi hàm lọc phải nằm trong một thư viện liên kết động (Dynamic Link Library). Cần phải gọi hàm hook toàn cục trong một DLL tách biệt với chương trình có cài đặt hàm hook. Chương trình phải có tham chiếu tới thư viện DLL trước khi có thể cài đặt hàm hook. Hàm LoadLibrary được sử dụng để lấy được tham chiếu tới một DLL. Khi đã có được tham chiếu, hàm GetProcAddress được sử dụng để lấy con trỏ tới hàm hook. Cuối cùng, hàm SetWindowsHookEx được gọi để cài đặt hàm hook trong hook chain tương ứng. Hàm sau để cài đặt sự kiện Hook.

```
void CMyDlg::OnHook(){
    if(hooked==true)
    {
        removehook();
        hooked = false;
    } else
    {
        installhook(this-
>GetSafeHwnd());
        hooked = true;
    m_hook.SetWindowText("UnHook
Keyboard");
    }
}
```

*Truyền nhận dữ liệu thu thập được*

Bộ giao thức TCP/IP được coi là ngôn ngữ chung của mạng Internet. Tất cả các hệ thống kết nối với Internet hiện nay đều được thiết kế dựa trên bộ giao thức này, cho phép các máy tính chạy trên các hệ điều hành khác nhau kết nối với nhau.

Server nghe ngóng để tiếp nhận các yêu cầu kết nối đến. Client thiết lập kết nối, gửi file đến Server. Mã nguồn cho kịch bản này cũng được cung cấp trong đĩa CD tại. TCP là giao thức đảm bảo hướng kết nối (Connection-oriented) tin cậy (Reliability), điều khiển luồng (Flow Control) để đảm bảo truyền dữ liệu đầy đủ và chính xác tới nơi nhận. Giao thức FTP hoạt động trên nền TCP ở tầng giao vận nên có khả năng truyền dữ liệu tới máy chủ tin cậy và chính xác



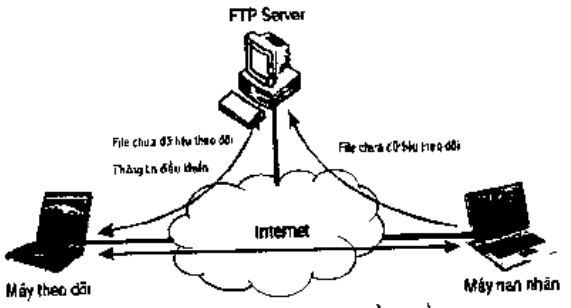

**Hình 2.** *Truyền dữ liệu bằng TCP Socket*

Ngoài kênh kết nối với FTP Server, còn có một kênh truyền để giao tiếp trực tiếp giữa máy điều khiển và máy bị theo dõi. Kết nối này cũng được xây dựng trên TCP socket để đảm bảo truyền thông tin cậy. Thông qua kênh truyền này, máy điều khiển sẽ gửi mã lệnh trực tiếp đến máy có chứa Keylogger

**Thử nghiệm phần mềm**

*Thiết lập môi trường thử nghiệm*

Phần mềm Keylogger được đính kèm vào một đường link, một người sử dụng máy tính truy cập Internet sẽ kích vào đường link được dẫn. Khi người sử dụng mở file, Keylogger sẽ bắt đầu hoạt động ngầm trong máy tính. FTP Server là máy chủ cung cấp dịch vụ truyền file để tiếp nhận dữ liệu do máy bị theo dõi truyền về. Máy theo dõi sẽ truy cập vào máy chủ để tải các file dữ liệu thu thập được.




**Hình 3.** *Mô hình hoạt động của phần mềm Keylogger*

*Thực thi chương trình Keylogger*

Mô hình hoạt động của hệ thống thử nghiệm được minh họa ở Hình 3. Modul chương trình Keylogger tại máy nạn nhân được thiết lập để được kích hoạt mỗi khi hệ thống được khởi động. Chương trình bắt đầu theo dõi mọi thao tác bàn phím, lưu thông tin thu thập được vào các tập tin log tại đường dẫn xác định trước. Sau mỗi khoảng thời gian được thiết lập trước, một luồng chương trình được kích hoạt gửi dữ liệu các tập tin tới máy chủ FTP Chương trình Keylogger mở một kênh truyền tới máy tính có chương trình điều khiển đang chờ đợi. Keylogger hoạt động ở chế độ nhận lệnh và gửi trả kết quả lại cho chương trình điều khiển.

Modul chương trình điều khiển tại máy theo dõi để điều khiển Keylogger từ xa, Khi bắt đầu ở chế độ lắng nghe (Listen), chương trình chờ các kết nối đến. Khi có kết nối đến, chương trình điều khiển chấp nhận kết nối và thông báo cho người dùng. Người sử dụng tương tác với Keylogger bằng các dòng lệnh nhập vào từ giao diện phần mềm điều khiển. Lệnh được gửi đến phần mềm theo dõi, nhận kết quả phản hồi hiển thị cho người sử dụng. Toàn bộ thông tin thu được từ bàn phím sẽ được gửi qua kết nối socket tới một FTP server có sẵn. Chủ sở hữu của phần mềm sẽ tương tác với phần mềm gián điệp qua server này Chương trình theo dõi không chỉ kết nối với chương chương trình điều khiển mà còn gửi tập tin log lên máy chủ FTP có địa chỉ được đặt trong mã nguồn của nó.

Các phần mềm diệt Virus hiện nay đều có cài đặt các chức năng theo dõi và tìm ra các phần mềm gián điệp như Keylogger. Vì vậy, để thử nghiệm khả năng hoạt động của phần mềm, chúng tôi cho Keylogger hoạt động ở các chế độ với các thông số khác nhau Bằng cách thay đổi tham số về khoảng thời gian cập nhật dữ liệu ra bên ngoài sẽ có các kịch bản hoạt động khác nhau.

**Bảng 1.** *Khả năng phát hiện Keylogger của một số phần mềm diệt Virus*

| Phần mềm | Kết quả |
|---|---|
| **t = 3600s** | |
| 360 Total Security | Không phát hiện được |
| VirusTotal | Không phát hiện được |
| BKAV | Không phát hiện được |
| Sophos | Không phát hiện được |
| **t = 1200s** | |
| 360 Total Security | Không phát hiện được |
| VirusTotal | Không phát hiện được |
| BKAV | Không phát hiện được |
| Sophos | Không phát hiện được |
| **t = 600s** | |
| 360 Total Security | Không phát hiện được |
| VirusTotal | Không phát hiện được |
| BKAV | Không phát hiện được |
| Sophos | Không phát hiện được |
| **t = 300s** | |
| 360 Total Security | Không phát hiện được |
| VirusTotal | Không phát hiện được |
| BKAV | Không phát hiện được |
| Sophos | Không phát hiện được |
| **t = 120s** | |
| 360 Total Security | Không phát hiện được |
| VirusTotal | Không phát hiện được |
| BKAV | Phát hiện được |
| Sophos | Phát hiện được |
| **t = 30s** | |
| 360 Total Security | Không phát hiện được |
| VirusTotal | Phát hiện được |
| BKAV | Phát hiện được |
| Sophos | Phát hiện được |
| **t = 10s** | |
| 360 Total Security | Phát hiện được |
| VirusTotal | Phát hiện được |
| BKAV | Phát hiện được |
| Sophos | Phát hiện được |

*Kết quả*

Sau khi chương trình Keylogger đã được kích hoạt, sử dụng chương trình điều khiển để thu dữ liệu, Toàn bộ thông tin nhận từ bàn phím được chuyển về FTP server, máy tính theo dõi truy cập và lấy được dữ liệu. Chúng tôi sử dụng một số phần mềm diệt Virus để quét và phát hiện Keylogger cài đặt trên máy. Tùy thuộc vào tham số chu kỳ cập nhật dữ liệu ra bên ngoài, các phần mềm diệt Virus có thể

không phát hiện được sự hiện diện của phần mềm Keylogger Bảng 1 minh họa kết quả thực nghiệm trực tiếp với các chu kỳ cập nhật dữ liệu khác nhau.

Bảng 1 cho thấy khi chu kỳ gửi dữ liệu ra ngoài càng nhỏ thì khả năng bị các phần mềm diệt Virus phát hiện càng cao. Điều này cho thấy việc giảm bớt tần suất cập nhật khiến cho việc phát hiện trở nên khó khăn hơn. Việc cập nhật dữ liệu thường xuyên sẽ cung cấp cho người theo dõi thông tin kịp thời, tuy vậy điều này làm tăng khả năng các phần mềm diệt Virus sẽ thu thập đủ chứng cứ để kết luận đó là phần mềm gián điệp.

## PHÁT HIỆN, LOẠI BỎ KEYLOGGER

### Dấu hiệu của Keylogger

Các đặc điểm hoạt động của Keylogger là cơ sở để phát hiện ra sự hiện diện của các phần mềm loại này trên máy bị nhiễm. Việc theo dõi hệ thống, nhận diện các hành vi bất thường là cách hiệu quả để phát hiện hoạt động của Keylogger. Đặc điểm nổi bật nhất của Keylogger thường xuyên gọi ngắt để theo dõi các sự kiện bàn phím do các ứng dụng gửi đến hệ điều hành. Keylogger định kỳ gửi dữ liệu thu được ra bên ngoài thông qua các giao thức TCP/IP Các biểu hiện sau đây có thể là dấu hiệu cho thấy có Keylogger đang hoạt động trên máy:

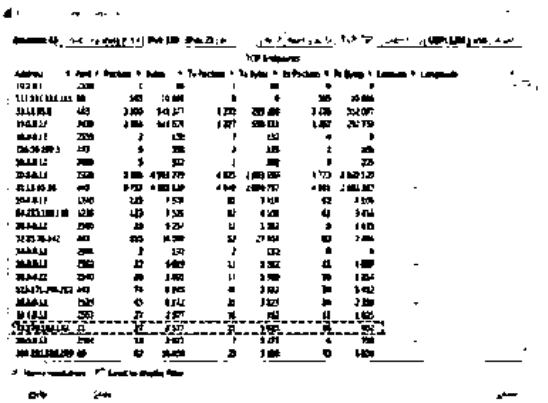
- Máy tính chạy chậm hơn so với tốc độ thông thường; Tốc độ gõ phím bị chậm lại tuy rằng không đáng kể.

- Xuất hiện file dữ liệu lạ trên máy tính, không thể đọc nội dung bằng các chương trình đọc text thông thường.

- Một số cổng TCP/IP được mở dù đã từng được đóng lại.

### Phát hiện và phòng chống Keylogger

Dựa vào các dấu hiệu hoạt động của Keylogger, có thể sử dụng một số công cụ để phát hiện ra phần mềm gián điệp như Task Manager hay Process Explorer. Các tiến trình có tên lạ, hoặc có tên gần giống với các công cụ của hệ điều hành nhưng trong phần mô tả không có thông tin rõ ràng có thể là Keylogger. Tuy vậy, một số phần mềm gián điệp có thể ẩn trước các chương trình này. Vì vậy các công cụ theo dõi tiến trình cũng chỉ được sử dụng trong một số trường hợp nhất định, ngoài ra cần có các kỹ thuật khác Kỹ thuật phân tích mã là quá trình theo dõi, phân tích mã nguồn chương trình từ đó rút ra được nguyên lý hoạt động, chức năng và nguồn gốc của chương trình để phát hiện và hạn chế tác hại của nó. Các công cụ theo dõi, giám sát tiến trình, lưu lượng mạng như TCPView, ProcessMon, Wireshark và các phần dịch ngược mã nguồn chương trình (Reverse Engineering) có thể được sử dụng để phát hiện Keylogger



**Hình 4**. *Wireshark hiển thị lưu thông mạng do Keylogger thiết lập*.

Một đặc điểm khác của Keylogger là cơ sở để nhận biết là các phần mềm dạng này phải truyền dữ liệu ra mạng bên ngoài sử dụng kỹ thuật lập trình socket Từ đặc điểm này, sử dụng các phần mềm Packet Sniffer để quan sát mạng như Wireshark sẽ giúp phân tích lưu lượng mạng và phát hiện các lưu lượng mạng bất thường. Sử dụng chức năng lọc trong các gói tin thỏa mãn một số điều kiện nhất định, Ví dụ đặt thuộc tính "IP address = 203 162.159 30" sẽ cho phép lọc luồng dữ liệu chứa tất cả các gói tin có địa chỉ IP nguồn hoặc IP đích là 203.162.159 30. Hình 4 hiển thị kết quả quan sát lưu lượng mạng khi chạy chương trình Keylogger. Khi đã phát hiện được các tiến trình Keylogger, sẽ tìm ra nơi chứa phần mềm và có thể loại bỏ được Keylogger.

## KẾT LUẬN

Từ các cơ sở lý thuyết về phần mềm theo dõi bàn phím chúng tôi xây dựng được một phần mềm có khả năng theo dõi các thao tác gõ

phím và gửi dữ liệu thu thập được cho chủ thể theo dõi qua các kết nối TCP socket. Chương trình có kích thước nhỏ gọn, có thể được đính kèm vào các file dữ liệu khác. Phần mềm có khả năng theo dõi bàn phím hiệu quả, gửi dữ liệu bí mật về địa chỉ được thiết lập sẵn. Qua thực nghiệm cho thấy việc gửi dữ liệu theo dõi được theo định kỳ sẽ giúp phần mềm Keylogger tránh bị các phần mềm diệt Virus phát hiện ra. Trên cơ sở các kỹ thuật phát hiện được đề xuất, hướng phát triển là áp dụng các kỹ thuật lập trình phân tích gói tin (sử dụng tcpdump) có ứng dụng các kỹ thuật học máy (Machine Learning) để tự động lọc các lưu thông mang nghi ngờ, từ đó phát hiện ra các phần mềm gián điệp.

## TÀI LIỆU THAM KHẢO


1. A Abalmasov (2013), *How to detect Keylogger and remove it from your computer*, Best Tips Tech.

2 M Chapple (2005), *How to detect and prevent Keylogger attacks*, Tech Targetk.

3 M. Curtin (1998), *Introduction to Network Security*.

4 M. Watkins (2008), *CCNA Security*, Cisco Press, 800 East 96th street

5 Dafydd Stuttard, Marcus Pinto (2011), *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd Edition, Wiley Publishing Inc

6. Mohammed J. Zaki, Wagner Meira Jr. (2014), *Data Mining and Analysis: Fundamental Concept and Algorithms*, Cambridge University Press

7 Stephen Northcutt, Donald McLachlan, Judy Novak (2000). *Network Intrusion Detection: An Analyst's Handbook*, 2nd Edition, New Riders.

8 Jan Killmeyer (2000), *Information Security Architecture: An Integrated Approach to Security in the Organization*, 1st Edition, CRC Press

9 Ryan Russell (2000), *Hack Proofing Your Network: Internet Tradecraft*, 1st Edition, CRC Press.

10. Stuart McClure (1999), *Hacking Exposed. Network Security Secrets & Solutions*, Computing Mcgraw-Hill

11 David J Marchette (2001), *Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint*, Springer Verlag.

12 Eric Maiwald (2012), *Network Security: A Beginner's Guide*, Osborne

13 David J Gunkel (2000), *Hacking Cyberspace*, Westview Press

14 Joel Scambray, Stuart McClure (2001), *Hacking Exposed Windows 2000*, McGraw-Hill

15. Thomas R Peltier (2001), *Information Security Risk Analysis*, Auerbach Publications

16. Jeff Crume (2000), *Inside Internet Security. What Hackers Don't Want You To Know*, Addison-Wesley.

17 Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L Cardash (2001), *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, Center for Strategic & Int'l Studies

18 Christopher King, Ertem Osmanoglu, Curtis Dalton (2001), *Security Architecture. Design, Deployment and Operations*, McGraw-Hill.


## SUMMARY

## DETECTING AND ELIMINATING KEYLOGGER


**Nguyen Dang Tien***

*People's Police University of Technology and Logistics, Bac Ninh, Vietnam*



Keylogger has been exploited widely and poses a serious security threat In this article, we introduced our proposed approach to detect and eliminate Keyloggers First, we design and implement a software Keylogger following basic principles Afterwards, we deploye it in a real life scenario to test its capability of spying victim computer Experimental results show that the software can effectively infiltrate into computers and secretly transfer data to a designated server without being detected by anti-Virus softwares Based on the activities of the software, we propose some solutions to detect and eventually eliminate Keylogger. For future work, we are working on the improvement of the Keylogger as well as the countermeasures We propose incorporating Machine Learning into the detection process, thereby increasing the overall performance



**Keywords:** *Information Security, Malware, Wireshark, Log file, Network traffic*

***Ngày nhận bài:02/3/2017; Ngày phản biện:09/3/2017; Ngày duyệt đăng: 31/5/2017***



* *Email: dangtient36@gmail.com*