HƯỚNG DẪN GỠ BỎ MÃ ĐỘC TRONG MÁY TÍNH BỊ NHIỄM

Đây là trường hợp đã biết chính xác máy nào bị nhiễm Botnet

LƯU Ý: Trước khi xóa bỏ file gì, hãy sao lưu trước khi xóa.

Tải bộ Tools của Microsoft tại:

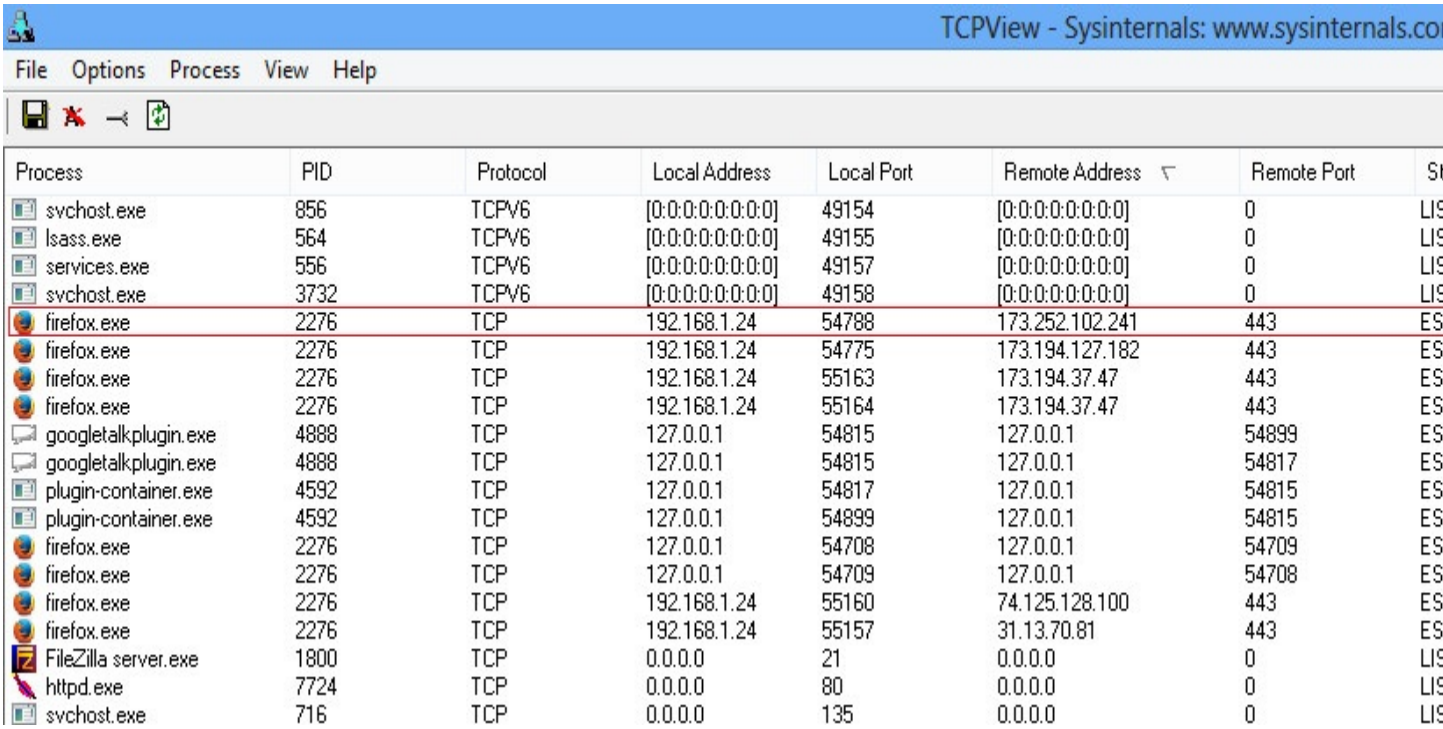
http://download.sysinternals.com/files/SysinternalsSuite.zip

1. **Hệ điều hành:**

   + Phần mềm trên chỉ chạy được trên hệ điều hành Windows.

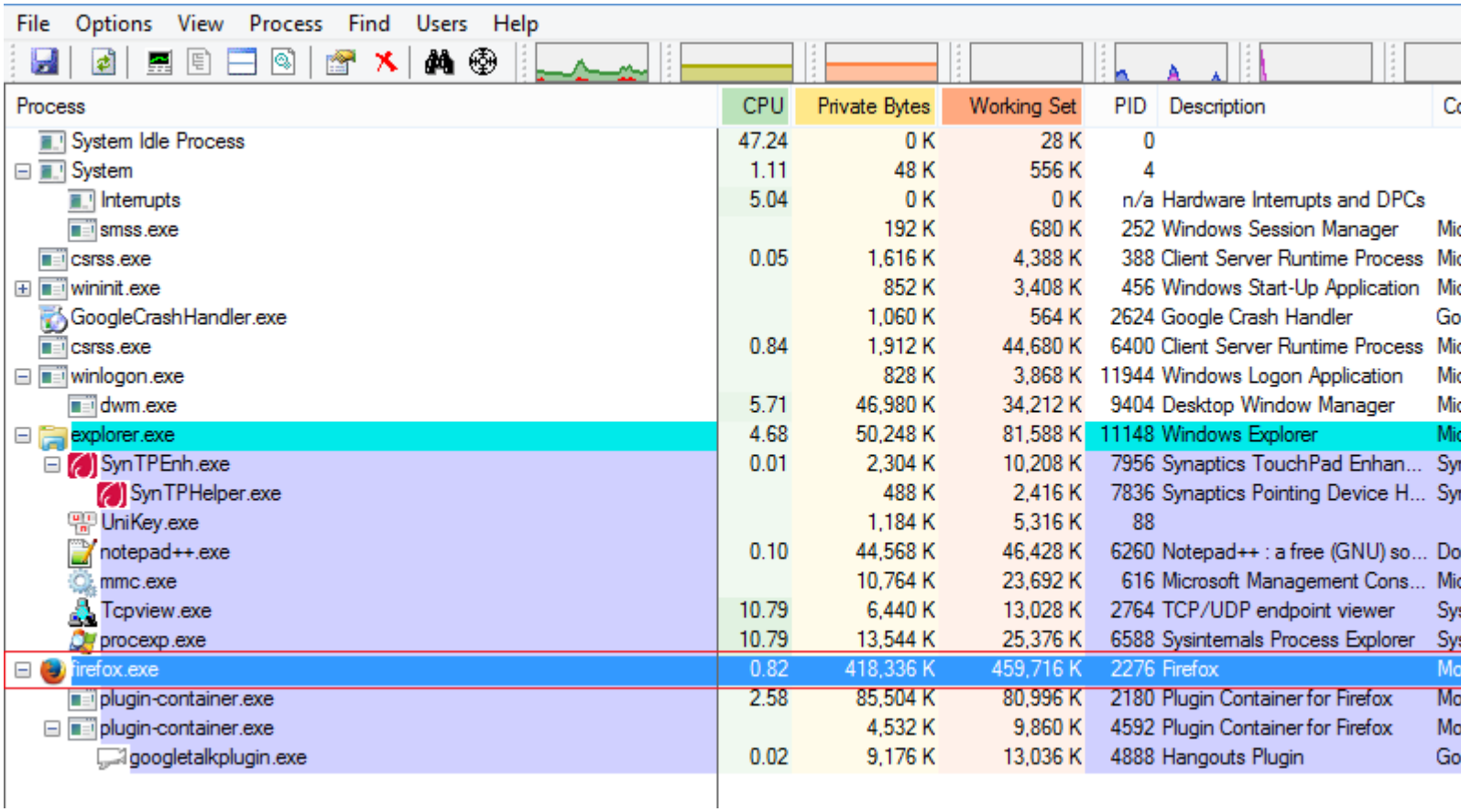
2. **Các kết nối hiện tại**:

   + Chạy chương trình ***TCPView.exe*** trong gói tải ở trên. Cho chạy rồi lưu lại xem tiến trình nào đang kết nối tới địa chỉ Đích đã cung cấp ở email. Ví dụ ở hình dưới, IP đích nếu là 173.252.102.241 thì tiến trình có tên firefox.exe đang nhiễm mã độc Botnet.



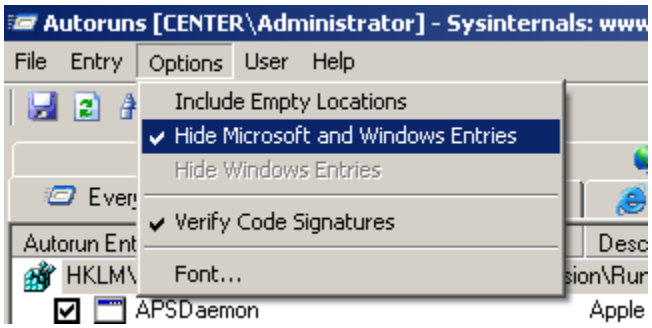
3. **Dừng/xóa các Process (tiến trình) đang chạy**:

Chạy file ***Procexp.exe*** trong gói tải ở trên. Như ở Ví dụ trên xác định tiến trình có PID=2276 thì click phải chuột và tiến hành "kill" tiến trình. Bước này nhằm xóa tiến trình đang chạy để xóa file bị nhiễm.



4. **Các Process sẽ khởi động cùng hệ thống**:

Chạy file ***Autoruns.exe*** trong gói tải về ở trên. Cho chạy hết (mất khoảng 1 phút) sau đó check vào các ***dấu check*** ở các dòng ***Options/Hide Microsoft and Windows Entries*** và ***Verify Code Signatures*** *(xem hình dưới)* sau đó F5. Những chương trình nào được ký (có chữ **Verified**) thì có thể bỏ qua, các chương trình nào có chữ **Not Verified** hoặc **không có chữ gì** thì là chương trình nghi ngờ mã độc. Để kiểm tra có thể copy các file này upload lên http://www.virustotal.com để kiểm tra. Nếu các Antivirus cho là Virus thì cần xóa bỏ tập tin này.

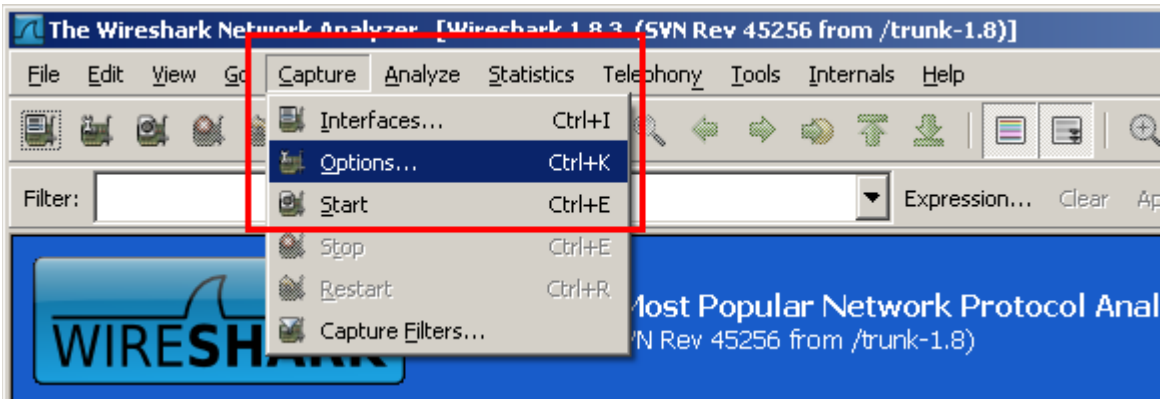


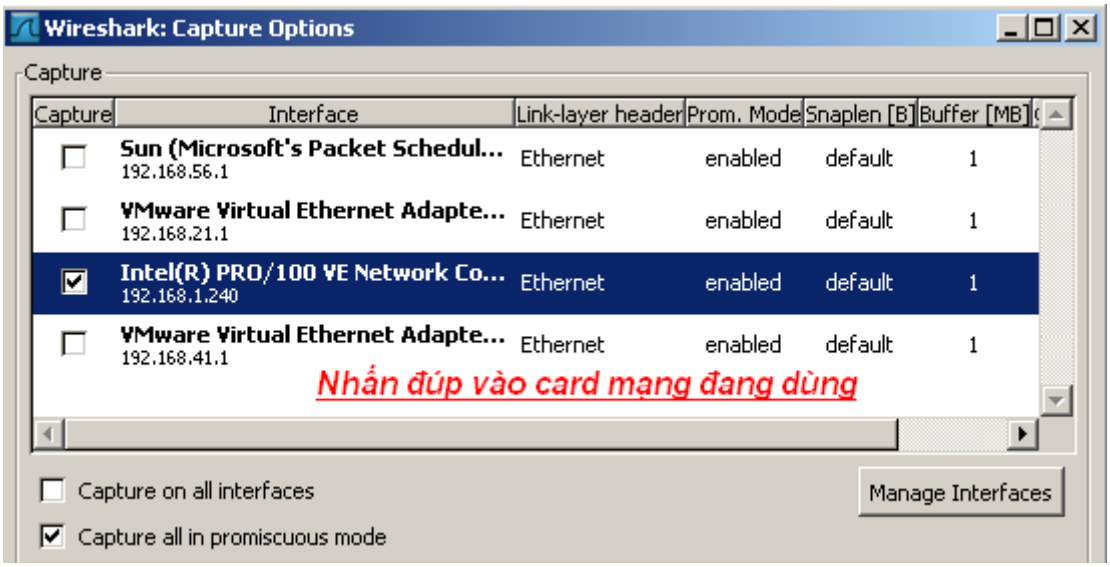
5. **Bắt gói tin bằng Wireshark**

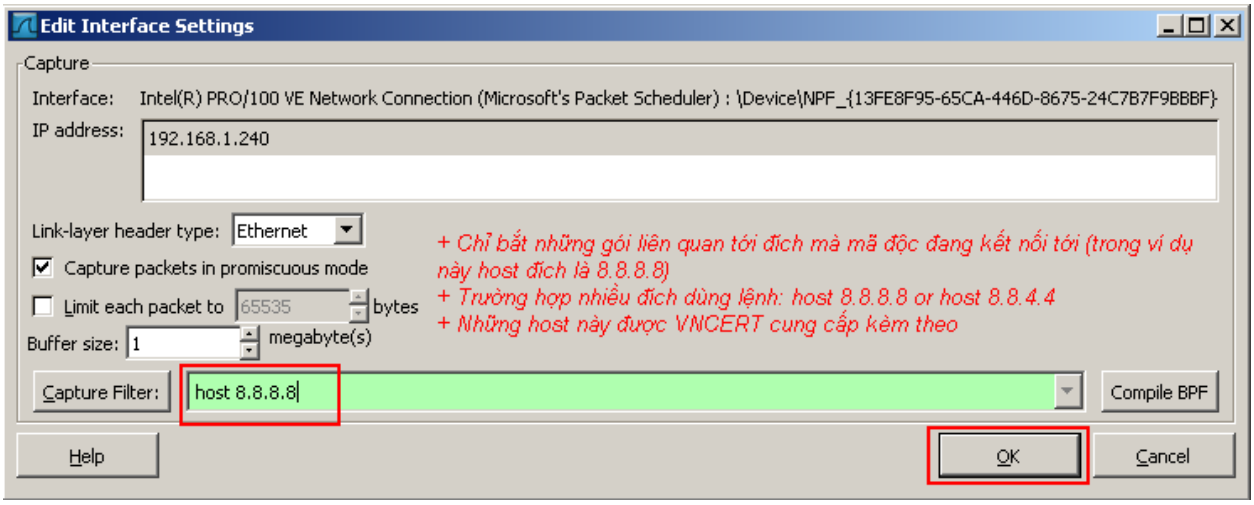
Đây là trường hợp kiểm tra chắc chắn máy tính đang kiểm tra tồn tại Mã độc tham gia mạng lưới Botnet. Để kiểm tra làm theo các bước:

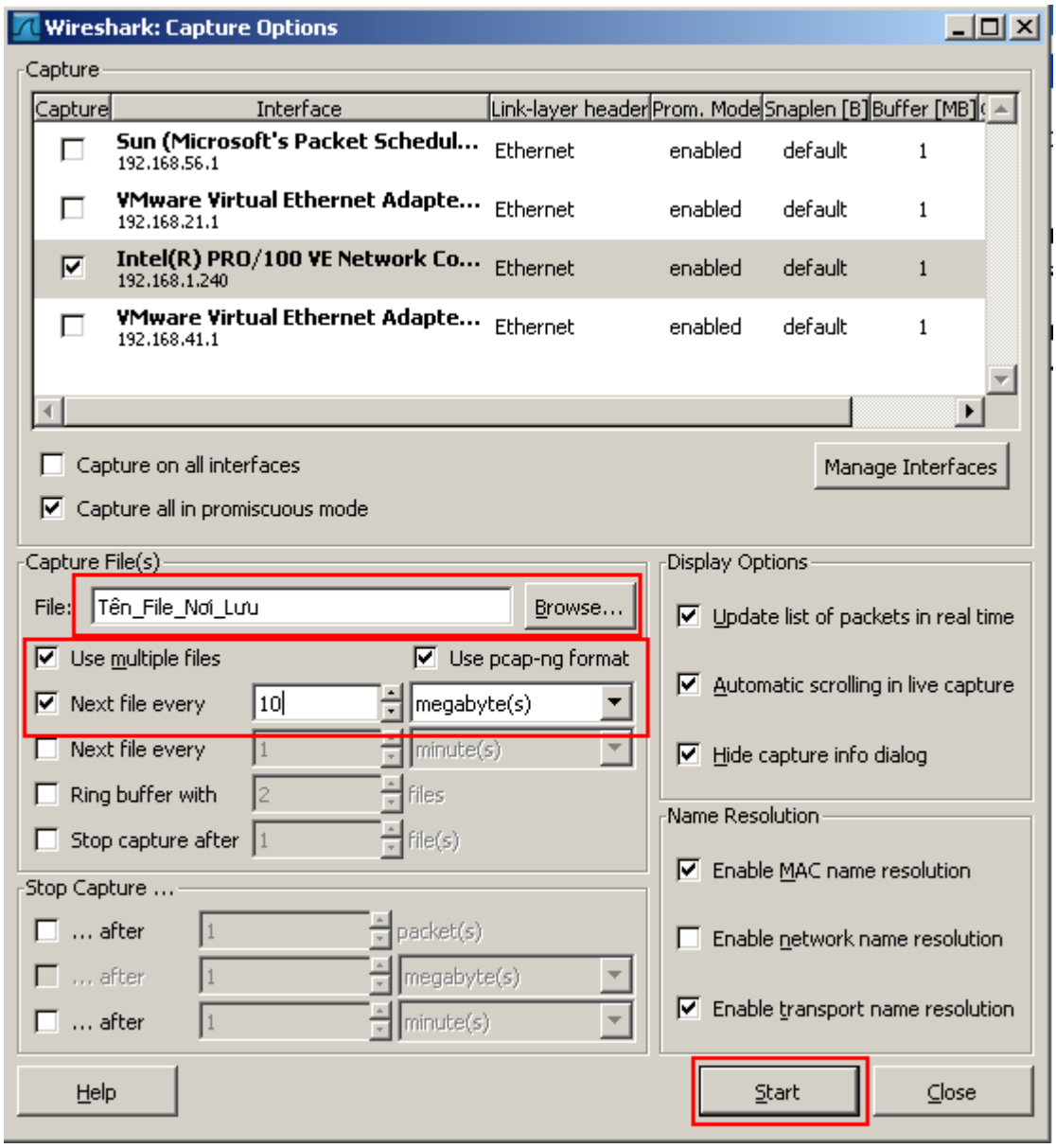
+ Cài đặt **Wireshark** được tải tại http://www.wireshark.org/download.html

+ Tiến hành bắt gói tin đang ra-vào trong máy. Xem hình dưới:




Wireshark: Capture Options
Capture
Capture
Interface
Link-layer header
Prom. Mode
Snaplen [B]
Buffer [MB]
Sun (Microsoft's Packet Schedul...
192.168.56.1
Ethernet
enabled
default
1
VMware Virtual Ethernet Adapte...
192.168.21.1
Ethernet
enabled
default
1
Intel(R) PRO/100 VE Network Co...
192.168.1.240
Ethernet
enabled
default
1
VMware Virtual Ethernet Adapte...
192.168.41.1
Ethernet
enabled
default
1
Nhấn đúp vào card mạng đang dùng
Capture on all interfaces
Manage Interfaces
Capture all in promiscuous mode


Edit Interface Settings
Capture
Interface:
Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : \Device\NPF_{13FE8F95-65CA-446D-8675-24C7B7F9BBBF}
IP address:
192.168.1.240
Link-layer header type:
Ethernet
Capture packets in promiscuous mode
Limit each packet to
65535
bytes
Buffer size:
1
megabyte(s)
+ Chỉ bắt những gói liên quan tới đích mà mã độc đang kết nối tới (trong ví dụ này host đích là 8.8.8.8)
+ Trường hợp nhiều đích dùng lệnh: host 8.8.8.8 or host 8.8.4.4
+ Những host này được VNCERT cung cấp kèm theo
Capture Filter:
host 8.8.8.8
Compile BPF
Help
OK
Cancel



+ Nhấn **Start** để bắt đầu quá trình bắt gói tin. Nên nhớ ở hình cuối cùng, nếu lưu lượng quá lớn thì nên **bỏ dấu check** ở ô có dòng "*Update list of packets in real time*".

+ Nếu **không có** gói tin nào thuộc lọc trên thì có thể cắm máy cho chạy trong vòng 12 tiếng.

+ Nếu **có gói tin** nào hiện lên thì chắc chắn máy đang có tiến trình nhiễm Botnet và đang kết nối ra ngoài. Quay lại dùng công cụ TCPView để xác định tên tiến trình và xóa bỏ.

*

* * *

Trong quá trình lấy thông tin nếu chưa rõ hoặc cần hỗ trợ thì có thể:

a. *Support qua Yahoo ID**: hatienkma***

b. *Số điện thoại: **0986.334.358***

c. *Email: hvtien@vncert.vn*