HƯỚNG DẪN GÕ 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.

<u> </u>				1	CPView - Sysinternals:	www.sysinterna	als.co					
File Options Process	File Options Process View Help											
🔛 🔺 🖾												
Process	PID	Protocol	Local Address	Local Port	Remote Address 🗸	Remote Port	S					
🔟 svchost.exe	856	TCPV6	[0:0:0:0:0:0:0:0]	49154	[0:0:0:0:0:0:0:0]	0	LIS					
🔝 Isass.exe	564	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LIS					
🔝 services.exe	556	TCPV6	[0:0:0:0:0:0:0:0]	49157	[0:0:0:0:0:0:0:0]	0	LIS					
🔝 svchost.exe	3732	TCPV6	[0:0:0:0:0:0:0:0]	49158	[0:0:0:0:0:0:0:0]	0	LIS					
🥘 firefox.exe	2276	TCP	192.168.1.24	54788	173.252.102.241	443	ES					
🥘 firefox.exe	2276	TCP	192.168.1.24	54775	173.194.127.182	443	ES					
🥘 firefox.exe	2276	TCP	192.168.1.24	55163	173.194.37.47	443	ES					
🥘 firefox.exe	2276	TCP	192.168.1.24	55164	173.194.37.47	443	ES					
💭 googletalkplugin.exe	4888	TCP	127.0.0.1	54815	127.0.0.1	54899	ES					
💭 googletalkplugin.exe	4888	TCP	127.0.0.1	54815	127.0.0.1	54817	ES					
plugin-container.exe	4592	TCP	127.0.0.1	54817	127.0.0.1	54815	ES					
plugin-container.exe	4592	TCP	127.0.0.1	54899	127.0.0.1	54815	ES					
📵 firefox.exe	2276	TCP	127.0.0.1	54708	127.0.0.1	54709	ES					
🥘 firefox.exe	2276	TCP	127.0.0.1	54709	127.0.0.1	54708	ES					
🧓 firefox.exe	2276	TCP	192.168.1.24	55160	74.125.128.100	443	ES					
🥘 firefox.exe	2276	TCP	192.168.1.24	55157	31.13.70.81	443	ES					
🔁 FileZilla server.exe	1800	TCP	0.0.0	21	0.0.0.0	0	LIS					
🔪 httpd.exe	7724	TCP	0.0.0	80	0.0.0.0	0	LIS					
🔟 svchost.exe	716	TCP	0.0.0	135	0.0.0.0	0	LIS					

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.

File Options View Process Find Users Help						
🛃 🖻 🚍 🖻 🍽 🖀 🗶 👫 🍪 💭						
Process	CPU	Private Bytes	Working Set	PID	Description	С
System Idle Process	47.24	0 K	28 K	0		
🖃 🔝 System	1.11	48 K	556 K	4		
Interrupts	5.04	0 K	0 K	n/a	Hardware Interrupts and DPCs	;
smss.exe		192 K	680 K	252	Windows Session Manager	Mie
CSrss.exe	0.05	1,616 K	4,388 K	388	Client Server Runtime Process	Mie
🕀 💽 wininit.exe		852 K	3,408 K	456	Windows Start-Up Application	Mie
🚯 GoogleCrashHandler.exe		1,060 K	564 K	2624	Google Crash Handler	Go
csrss.exe	0.84	1,912 K	44,680 K	6400	Client Server Runtime Process	Mie
🖃 📰 winlogon.exe		828 K	3,868 K	11944	Windows Logon Application	Mie
dwm.exe	5.71	46,980 K	34,212 K	9404	Desktop Window Manager	Mie
🖃 🚞 explorer.exe	4.68	50,248 K	81,588 K	11148	Windows Explorer	Mie
🖃 🏉 Syn TPEnh.exe	0.01	2,304 K	10,208 K	7956	Synaptics TouchPad Enhan	Sy
Syn TPHelper.exe		488 K	2,416 K	7836	Synaptics Pointing Device H	Sy
💮 UniKey.exe		1,184 K	5,316 K	88		
Notepad++.exe	0.10	44,568 K	46,428 K	6260	Notepad++ : a free (GNU) so	. Do
, mmc.exe		10,764 K	23,692 K	616	Microsoft Management Cons	Mie
🔏 Tcpview.exe	10.79	6,440 K	13,028 K	2764	TCP/UDP endpoint viewer	Sy
🖉 procexp.exe	10.79	13,544 K	25,376 K	6588	Sysinternals Process Explorer	Sy
🖃 🎒 jirefox.exe	0.82	418,336 K	459,716 K	2276	Firefox	Мо
plugin-container.exe	2.58	85,504 K	80,996 K	2180	Plugin Container for Firefox	Мо
🖃 🔳 plugin-container.exe		4,532 K	9,860 K	4592	Plugin Container for Firefox	Mo
💭 googletalkplugin.exe	0.02	9,176 K	13,036 K	4888	Hangouts Plugin	Go
I	1					

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:

The Wireshark Network Analyzer [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]								
<u>File E</u> dit <u>V</u> iew <u>G</u> o		<u>Capture</u> <u>Analyze</u>	Statistics Tele	ephony <u>T</u> ools Internals <u>H</u> elp				
		💐 Interfaces	Ctrl+I	L @ @ @ 7 L E E O				
	_	👹 Options	Ctrl+K					
Filter:		🗐 <u>S</u> tart	Ctrl+E	Expression Clear Ap				
		🕷 Stop	Ctrl+E					
1		🕷 <u>R</u> estart	Ctrl+R	fact Dopular Natwork Dratacal Anal				
WIRESI		😹 Capture <u>F</u> ilters		N Rev 45256 from /trunk-1.8)				
	- 1							

Л	Wireshark: Capture Options									
ſ	apture –									
	Capture	Interface	Link-layer hea	der Prom. Mode S	naplen [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				
		<u>Nhân đúp và </u>	o card mạ	ng đang dù	ng	_				
	Capture on all interfaces Manage Interfaces									
	Capture all in promiscuous mode									

📶 Edit Inter	face 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 he Capture Limit eac Buffer size:	eader type: Ethernet ▼ + Chỉ bắt những gói liên quan tới đích mà mã độc đang kết nối tới (trong ví dụ packets in promiscuous mode này host đích là 8.8.8.8) th packet to 65535 → bytes 1 → megabyte(s) + 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 Fil	Iter: host 8.8.8.8 Compile BPF
Help	<u>OK</u> <u>C</u> ancel

📶 Wiresha	ark: Capture	Options						_	
Capture —									
Capture		Interface		Link-layer head	er Prom.	Mode	5naplen [B]	Buffer [MB	3
	iun (Microso 92.168.56.1	ft's Packet Sc	hedul	Ethernet	ena	bled	default	1	
	'Mware Virt u 92.168.21.1	ual Ethernet A	dapte	Ethernet	ena	bled	default	1	
	ntel(R) PRO 92.168.1.240	/100 VE Netwo	ork Co	Ethernet	ena	bled	default	1	
	Mware Virtu 92.168.41.1	ual Ethernet A	dapte	Ethernet	ena	bled	default	1	
									<u> </u>
🔲 Captu	ure on all inter	faces					Man	age Interfa	ices
🔽 Captu	ure all in promi	scuous mode							
	Capture File(s)Display Options								
File: Tên_File_Nơi_Lưu Browse Image: Update list of packets in real time								l time	
🔽 Use mu	Use multiple files Vise pcap-ng format								
✓ Next file every 10 → megabyte(s) ✓ Automatic scrolling in live capture								pture	
Next file every 1 minute(s)									
📃 Ring bi	uffer with	2 -	files		Nam	ne Reso	lution		
🔲 Stop c	apture after	1 -	file(s)						
Stop Captur	re					Enable	e <u>M</u> AC nam	ie resolutior	ו
🔲 afte	er 1	×	packet(s)			Enable	e <u>n</u> etwork i	name resolu	ution
🗖 afte	er 1	×	megabyt	e(s)					h abia a
🔲 afte	er 1	× *	minute(s)) 🔻		chable	e gransport	. name reso	lucion
Help					[<u>5</u>	tart	⊆los	e

+ 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*