HƯỚNG DẪN XÁC ĐỊNH KHOANH VÙNG MÁY TÍNH NHIỄM MÃ ĐỘC

Trường hợp này áp dụng cho địa chỉ IP được dùng bởi nhiều máy con, ví dụ IP được dùng cho LAN truy cập Internet,...

Các trường hợp được hướng dẫn có sơ đồ mạng thuộc các trường hợp:

1. Tất cả máy con sử dụng IP đi qua máy cài đặt các dịch vụ DNS, ISA, IPTABLES,...

2. Tất cả máy con sử dụng IP đi qua ROUTER, SWITCH có cổng MONITOR, SPAN.

3. Trường hợp khác.

TRƯỜNG HỢP 1: Số lượng máy con lớn hơn 10 và tất cả máy con đi qua máy tính cài đặt dịch vụ nào đó. Ví dụ DNS, ISA, IPTABLES,...

- 1. Đối với Hệ điều hành Windows (ISA, DNS,...):
 - + Cài đặt Wireshark được tải tại http://www.wireshark.org/download.html

+ Tiến hành bắt gói tin đi qua máy này. Xem hình dưới:

📶 The Wireshark Ne	 .	ork Analyzer [Wir	ochaelz 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>A</u> nalyze	Statistics Tele	phon <u>y T</u> ools <u>I</u> nternals <u>H</u> elp
		😹 Interfaces	Ctrl+I	L @ @ @ 7 L 0
	_	🍯 Options	Ctrl+K	
Filter:		🗐 <u>S</u> tart	Ctrl+E	Expression Clear Ap
		🕷 Stop	Ctrl+E	
Λ		💓 <u>R</u> estart	Ctrl+R	Aget Dopular Network Protocol Anal
WIRESE	ī	😹 Capture <u>F</u> ilters		N Rev 45256 from /trunk-1.8)

1	U Wiresł	nark: Capture Options				<u> </u>
٢	Capture -					
	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	_
						• •
	🔲 Cap	ture on all interfaces			Man	age Interfaces
	🗹 Cap	ture 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

🕂 Wirest	hark: Capture	Options						_	
Capture -									
Capture		Interface		Link-layer head	der Pro	m. Mode	Snaplen [B]	Buffer [MB]	
	Sun (Microso 192.168.56.1	oft's Packel	t Schedul	Ethernet	е	nabled	default	1	
	VMware Virt 192.168.21.1	ual Etherne	t Adapte	Ethernet	е	nabled	default	1	
	Intel(R) PRO 192.168.1.240)/100 ¥E Ne	twork Co	Ethernet	е	nabled	default	1	
	VMware Virt 192.168.41.1	ual Etherne	t Adapte	Ethernet	е	nabled	default	1	
								<u> </u>	
🔲 Cap	ture on all inte	rfaces					Mana	age Interfac	ces
🗹 Cap	ture all in prom	iscuous mode	9						_
	-1 ()								
-Capture F	-ile(s)			_	٦٢	isplay Op	tions		
File: T	ên_File_Nơi_Lu	ບ		Browse		🗹 Upda	te list of pac	kets in real:	time
🗹 Use	<u>m</u> ultiple files		🔽 Use	pcap-ng forma	t	. Autor	a a bia a avallia	a ia liva ana	-
🗹 Next	: file every	10	🗧 megaby	te(s) 💆	<u> </u> '	✓ <u>A</u> utoi	nacie seroiiin	iy in iive cap	Jure
Next	: file every	1	minute(s) 💌	ון	✓ Hide	capture info	dialog	
🔲 Ring	buffer with	2	🗧 files			ame Rec	olution		
🔲 Stop	capture after	1	▲ file(s)				olacion		
Stop Capl	ture					🗸 Enab	le <u>M</u> AC name	e resolution	
🗖 a	fter 1		× packet(s)		_	Enab	le <u>n</u> etwork n	ame resolut	tion
🗖 a	fter 1		- megabyt	e(s)	<u> </u>				
🗖 a	fter 1		minute(s)) _	<u> </u>	♥ Enabi	ie <u>t</u> ransport	name resol	ucion
Help							ōtart	⊆lose	•

+ 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 chỉ cần bắt trong vòng 10 phút. Địa chỉ IP con đang thực hiện kết nối chính là IP nhiễm Botnet.

2. Đối với Hệ điều hành Linux (IPTABLES, DNS,...):

+ Kết nối vào SSH hoặc đăng nhập trực tiếp trên máy đó với quyền root.

+ Nếu chưa cài đặt tcpdump thì dùng lệnh "yum –y install tcpdump" để cài.

+ Nếu đã cài (đa số đã cài) tcpdump thì dùng lệnh sau để bắt gói tin

"tcpdump -w sniff.pcap -s0 dst 113.160.38.4".

Trong đó 113.160.38.4 là host. Địa chỉ này VNCERT sẽ cung cấp trong quá trình cảnh báo.

Sau 15 phút nhấn Ctrl + C để thoát và tiến hành phân tích. Nếu có máy con kết nối tới địa chỉ đích đã cung cấp thì địa chỉ máy đó chính là địa chỉ máy tính bị nhiễm.



<u>TRƯỜNG HỢP 2</u>: Số lượng máy con lớn hơn 10 và tất cả máy con đi qua ROUTER hay SWITCH có cổng MONITOR hay SPAN.

Cổng MONITOR hay SPAN là cổng mà có nhiệm vụ giữ 1 bản copy của các gói tin đi ra vào trong Switch.

+ Trường hợp này là phổ biến. Cách cấu hình phải là người am hiểu về kỹ thuật. Ví dụ dưới đây hướng dẫn cấu hình Switch.

+ Login vào quản lý Switch có giao diện (các loại khác tương tự).

System	Swi	tch Statı	ıs		Refresh H	elp	
Switch Status							
IP Access List	Prod	uct Name		FS726T			
- Set up	Firm	ware Versio	n	V1.2.3_02			
- <u>Set-up</u>	Prote	ocol Version	1	2.001.002			
Password	DHCF)		Disable			
Switch	IP ad	dress		192.168.1.9			
Port Configuration	Subn	et mask		255.255.255	.0		
- Statistics	Defa	ult gateway		192.168.1.10)		
- <u>Statistics</u>	MAC	address		00-14-6c-e5	-b9-9b		
• <u>QoS</u>	Syste	em Name		VNCERT			
VLAN	Loca	tion Name		Nghiep Vu			
Trunking	Logir	n Timeout (r	ninutes)	5			
Monitor	Syste	em UpTime		2 days 15 ho	ours 58 mins 55 seconds		
Advanced							
<u>Spanning Tree</u> <u>SNMP Configuration</u>	POF	RT Status	3				
IGMP Snooping Status Static Multicast Groups	ID	Speed	Flow Control	Link Status	Port Description	ID	
Port Rate Setting	10/	100 Mbp	s				
Storm Control	01	Auto	On	100M Full		02	A
	03	Auto	l∩n	100M Full		04	A

+ Ví dụ lấy cổng số 25 trên Switch làm cổng Monitor:

Monitor Setting

Group 1	Sniffer Mode	Bo	th	•										
	Sniffer Port	25	•											
	Source Port	01	02	03	04	05	06	07	08	09	10	11	12	13
			\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	◄	✓	◄	\checkmark	◄	◄	
		14	15	16	17	18	19	20	21	22	23	24	25	26
			\checkmark	~	~	\checkmark	~	~	•	~	\checkmark	•		
										_		_		
											Appl	ly	Ηe	elp

+ Sau khi cấu hình xong, nhìn vào Switch (hình dưới) chúng ta nối dây mạng vào cổng 25 và một máy tính có cài đặt Wireshark. Tiến hành bắt gói tin trên Wireshark theo hướng dẫn hình dưới.



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

📶 The Wireshark Ne	twork Analyzer [Wired	achark 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>A</u> nalyze <u>S</u> t	<u>Statistics Telephony Tools Internals H</u> elp
	🔉 🚉 Interfaces	Ctrl+I 🔍 🧔 🤿 🦚 🐺 🧏 🗐 🕞 🖸
	📕 🏭 Options	Ctrl+K
Filter:	🕮 <u>S</u> tart	Ctrl+E Expression Clear A
	🕷 Stop	Ctrl+E
Λ	🕍 <u>R</u> estart	Ctriffer Jost Dopular Network Protocol Apa
WIRESE	🛛 🖼 Capture Eilters	'N Rev 45256 from /trunk-1.8)
	Learning	

+ Tiến hành	bắt gói ti	in đi qua	máy này.	Xem hì	nh dưới:
				-	

🕂 Wir	rest	nark: Capture Options			_ 🗆	×
Captu	Jre-					
Capt	:ure	Interface	Link-layer l	neader Prom. Mode Snapl	len [B] Buffer [MB] 🤇 🖉	•
		Sun (Microsoft's Packet Schedul 192.168.56.1	Ethernet	enabled def	ault 1	
		VMware Virtual Ethernet Adapte 192.168.21.1	Ethernet	enabled def	ault 1	
	•	Intel(R) PRO/100 VE Network Co 192.168.1.240	Ethernet	enabled def	ault 1	
		VMware Virtual Ethernet Adapte 192.168.41.1	Ethernet	enabled def	ault 1	
		<u>Nhân đúp và </u>	o card r	nạng đang dùng	!	-
	Сар	ture on all interfaces			Manage Interfaces	
	Сар	ture all in promiscuous mode				

📶 Edit Interf	ace Settings	
Capture Interface: IP address:	Intel(R) PRO/100 VE Network Conn 192.168.1.240	ection (Microsoft's Packet Scheduler) : \Device\NPF_{13FE8F95-65CA-446D-8675-24C7B7F9BBBF}
Link-layer he Capture Limit each Buffer size:	ader type: Ethernet packets in promiscuous mode h packet to 65535 bytes t megabyte(s)	+ Chỉ bắt những gói liên quan tới địch mà mã độc đang kết nối tới (trong ví dụ này host địch là 8.8.8) + Trường hợp nhiều địch dùng lệnh: host 8.8.8 or host 8.8.4.4 + Những host này được VNCERT cung cấp kèm theo
Capture Filt	er: host 8.8.8.8	Compile BPF

🕂 Wiresl	hark: Capture	Options						۱×
Capture -								
Capture		Interface		Link-layer head	er Prom. M	ode Snaplen [I	BBuffer [MB]	
	Sun (Microso 192.168.56.1	oft's Packet	Schedul	Ethernet	enable	ed default	1	
	VMware Virt 192.168.21.1	ual Etherne	t Adapte	Ethernet	enable	ed default	1	
	Intel(R) PRO 192.168.1.240	/100 ¥E Ne	twork Co	Ethernet	enable	ed default	1	
	VMware Virt 192.168.41.1	ual Etherne	t Adapte	Ethernet	enable	ed default	1	
								-
🔲 Cap	ture on all inter	faces				Ma	nage Interface	s
🗹 Cap	ture all in prom	iscuous mode	•					_
Conture P	Filo(c)				Dicolas	Options		
	lie(s)			_		/ Options		
File:	ën_File_Noi_Lu	u		Browse	. 🗹 🛛	pdate list of p	ackets in real ti	ime
🗹 Use	<u>m</u> ultiple files		🔽 Use	pcap-ng format				
🔽 Next	t file every	10	🗧 megaby	rte(s) 💌		utomatic scrol	ling in live captu	ure
Next	t file every	1	minute(s) 💌	🛛 🗹 н	ide capture ini	fo dialog	
🔲 Ring	buffer with	2	🕂 files			Deselation		
🔲 Stop	capture after	1	file(s)		Ivame	Resolution —		
Stop Cap	ture	,			- E	nable <u>M</u> AC nai	me resolution	
🔲 а	fter 1		r packet(s)		E E	nable <u>n</u> etwork	name resolutio	n
🔲 а	fter 1		🗧 megabyt	e(s) 💌				
П а	fter 1		minute(s))	EI	nable <u>t</u> ranspoi	rt name resolut	ion
Help	b					<u>S</u> tart	⊆lose	

+ 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 chỉ cần bắt trong vòng 10 phút. Địa chỉ IP con đang thực hiện kết nối chính là IP nhiễm Botnet.

TRƯỜNG HỢP 3: Trường hợp khác

Đối với trường hợp khác bao gồm không có các thiết bị trên hoặc cùng chung LAN, chúng ta sử dụng ARP Spoofing nhằm giả mạo địa chỉ IP gateway và điều hướng tất cả các máy trong LAN đi qua một địa chỉ máy đã giả mạo. Chi tiết xem tại video hướng dẫn: <u>http://www.youtube.com/watch?v=4ZmYa_3UCVw</u>

Notice: Thông tin hỗ trợ khác.



