個案分析-

Y大學之 UDP Flood 攻擊事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

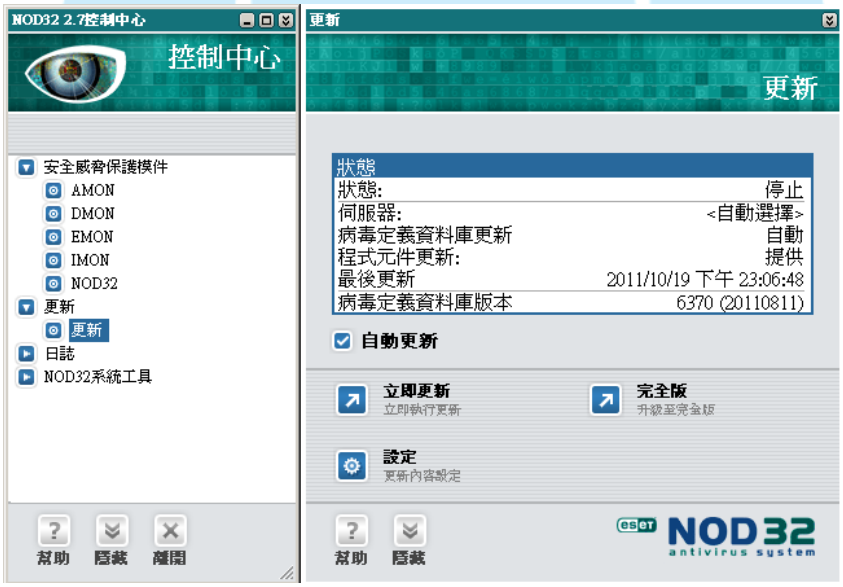
2014/06

一. 事件簡介

1. Y 大學電算中心資安人員發現某系所 IP 的網路流量異常的大，隨即遭受網路封鎖。
2. 資安人員通知本單位 TACERT 前往協助資安鑑識處裡。
3. 該感染主機為一台網頁伺服器，並具有網路硬碟分享功能讓其他有權限者能夠存取。

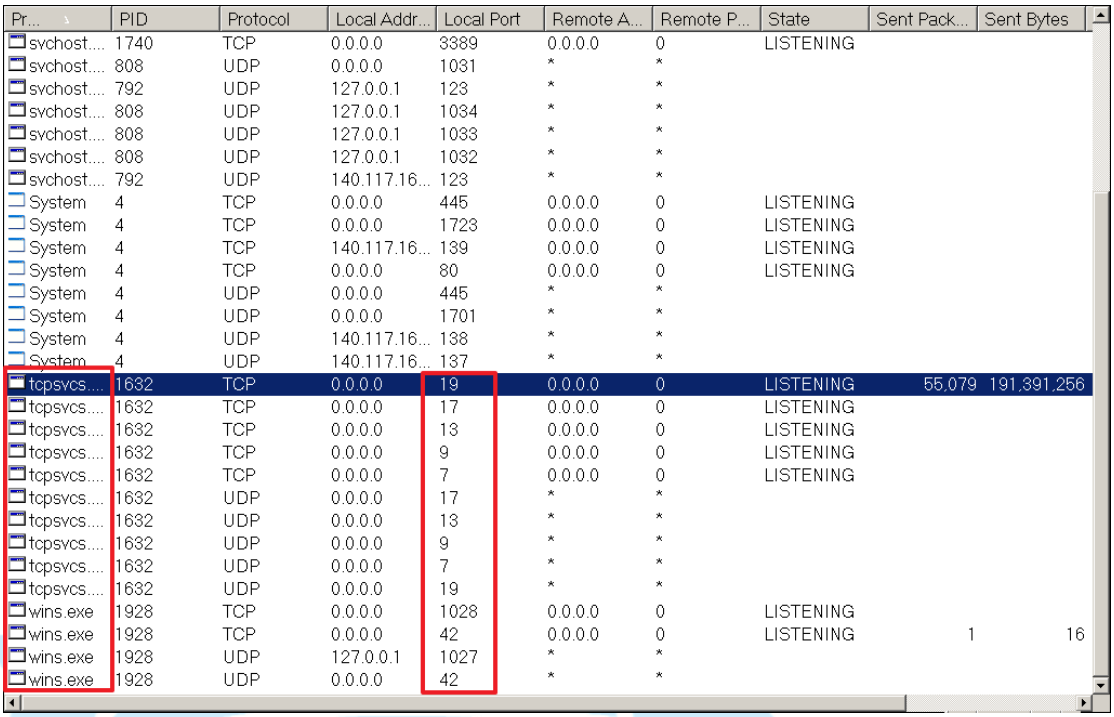
二. 事件檢測

1. 該主機的作業系統是 Windows Server 2003 版本。
2. 有安裝防毒軟體 NOD32，但是病毒碼最後更新是 2011 年，且無法再自動更新，為停止運作狀態。



3. 該主機有開啟遠端桌面連線功能，且管理者帳戶密碼設定的相當簡單為「12345」，故被破解機率登入極高。
4. 透過 TCPVIEW 的網路埠號監控軟體發現，有相當多的 TCP 或

UDP PORT 是被開啟的，可能被駭客利用來做網路攻擊行為。

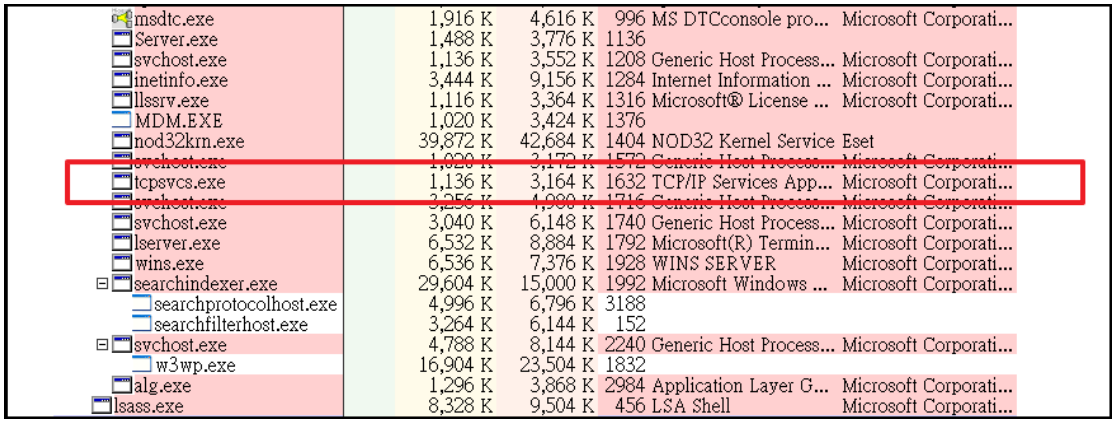


Pr...	PID	Protocol	Local Addr...	Local Port	Remote A...	Remote P...	State	Sent Pack...	Sent Bytes
svchost....	1740	TCP	0.0.0.0	3389	0.0.0.0	0	LISTENING		
svchost....	808	UDP	0.0.0.0	1031	*	*			
svchost....	792	UDP	127.0.0.1	123	*	*			
svchost....	808	UDP	127.0.0.1	1034	*	*			
svchost....	808	UDP	127.0.0.1	1033	*	*			
svchost....	808	UDP	127.0.0.1	1032	*	*			
svchost....	792	UDP	140.117.16...	123	*	*			
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING		
System	4	TCP	0.0.0.0	1723	0.0.0.0	0	LISTENING		
System	4	TCP	140.117.16...	139	0.0.0.0	0	LISTENING		
System	4	TCP	0.0.0.0	80	0.0.0.0	0	LISTENING		
System	4	UDP	0.0.0.0	445	*	*			
System	4	UDP	0.0.0.0	1701	*	*			
System	4	UDP	140.117.16...	138	*	*			
System	4	UDP	140.117.16...	137	*	*			
tcpsvcs....	1632	TCP	0.0.0.0	19	0.0.0.0	0	LISTENING	55,079	191,391,256
tcpsvcs....	1632	TCP	0.0.0.0	17	0.0.0.0	0	LISTENING		
tcpsvcs....	1632	TCP	0.0.0.0	13	0.0.0.0	0	LISTENING		
tcpsvcs....	1632	TCP	0.0.0.0	9	0.0.0.0	0	LISTENING		
tcpsvcs....	1632	TCP	0.0.0.0	7	0.0.0.0	0	LISTENING		
tcpsvcs....	1632	UDP	0.0.0.0	17	*	*			
tcpsvcs....	1632	UDP	0.0.0.0	13	*	*			
tcpsvcs....	1632	UDP	0.0.0.0	9	*	*			
tcpsvcs....	1632	UDP	0.0.0.0	7	*	*			
tcpsvcs....	1632	UDP	0.0.0.0	19	*	*			
wins.exe	1928	TCP	0.0.0.0	1028	0.0.0.0	0	LISTENING		
wins.exe	1928	TCP	0.0.0.0	42	0.0.0.0	0	LISTENING	1	16
wins.exe	1928	UDP	127.0.0.1	1027	*	*			
wins.exe	1928	UDP	0.0.0.0	42	*	*			

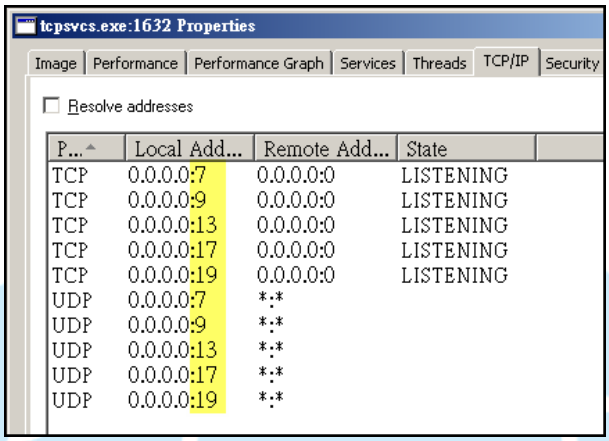
A. 原本的 Port 80 和 443 為網頁伺服器所使用。其他的 Port 7、9、13、17、19 等連接埠疑似為惡意程式 tcpsvcs.exe 所使用。

B. 其中 TCP port 19 正在發送大量的資料出去，因為登入的帳號權限不足或系統異常，tcpview 似乎無法看到正在連接的 IP。

C. 從程式管理工具來看 tcpsvcs.exe 的記憶體及 CPU 使用率並不高，但觀察其通訊埠的使用狀況就能發現異常，因為同時啟用了 TCP 和 UDP 的各五個 Port。



msdtc.exe	1,916 K	4,616 K	996	MS DTCconsole pro...	Microsoft Corporati...
Server.exe	1,488 K	3,776 K	1136		
svchost.exe	1,136 K	3,552 K	1208	Generic Host Process...	Microsoft Corporati...
inetinfo.exe	3,444 K	9,156 K	1284	Internet Information ...	Microsoft Corporati...
llssrv.exe	1,116 K	3,364 K	1316	Microsoft® License ...	Microsoft Corporati...
MDM.EXE	1,020 K	3,424 K	1376		
nod32krn.exe	39,872 K	42,684 K	1404	NOD32 Kernel Service	Eset
svchost.exe	1,020 K	3,172 K	1572	Generic Host Process...	Microsoft Corporati...
tcpsvcs.exe	1,136 K	3,164 K	1632	TCP/IP Services App...	Microsoft Corporati...
svchost.exe	3,256 K	4,980 K	1716	Generic Host Process...	Microsoft Corporati...
svchost.exe	3,040 K	6,148 K	1740	Generic Host Process...	Microsoft Corporati...
lserver.exe	6,532 K	8,884 K	1792	Microsoft(R) Termin...	Microsoft Corporati...
wins.exe	6,536 K	7,376 K	1928	WINS SERVER	Microsoft Corporati...
searchindexer.exe	29,604 K	15,000 K	1992	Microsoft Windows ...	Microsoft Corporati...
searchprotocolhost.exe	4,996 K	6,796 K	3188		
searchfilterhost.exe	3,264 K	6,144 K	152		
svchost.exe	4,788 K	8,144 K	2240	Generic Host Process...	Microsoft Corporati...
w3wp.exe	16,904 K	23,504 K	1832		
alg.exe	1,296 K	3,868 K	2984	Application Layer G...	Microsoft Corporati...
lsass.exe	8,328 K	9,504 K	456	LSA Shell	Microsoft Corporati...



tcpsvcs.exe:1632 Properties

Image | Performance | Performance Graph | Services | Threads | TCP/IP | Security

Resolve addresses

P...	Local Add...	Remote Add...	State
TCP	0.0.0.0:7	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9	0.0.0.0:0	LISTENING
TCP	0.0.0.0:13	0.0.0.0:0	LISTENING
TCP	0.0.0.0:17	0.0.0.0:0	LISTENING
TCP	0.0.0.0:19	0.0.0.0:0	LISTENING
UDP	0.0.0.0:7	*:*	
UDP	0.0.0.0:9	*:*	
UDP	0.0.0.0:13	*:*	
UDP	0.0.0.0:17	*:*	
UDP	0.0.0.0:19	*:*	

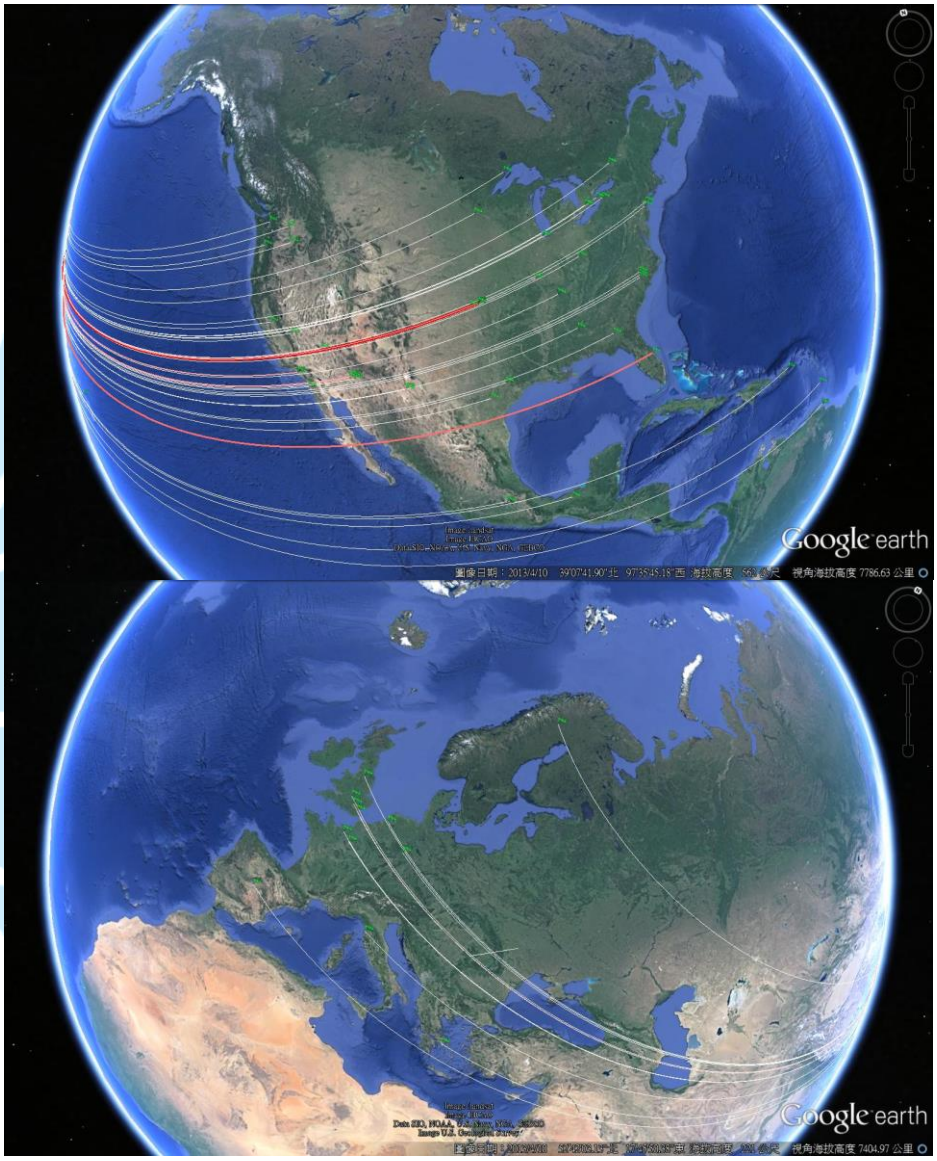
D. 將 tcpsvcs.exe 上傳至 Virustotal 檢測，並無檢測出任何惡意程式，因為此程式為 windows 系統內建的檔案，主要用在 DHCP server 的服務。

E. 觀察封包的側錄狀況得知，會造成大量網路流量的原因是 UDP Flooding，該主機 port 19 在短時間接收來自各地 IP 的 UDP 封包，導致頻寬阻塞。

a. 目前來看封包數多寡的 IP 依序為，50.89.131.39、76.91.29.198、108.211.6.11、108.221.6.111、68.229.1.208、174.26.24.179、107.214.80.227、108.237.253.48、98.167.148.250 等五十個以上不同

IP。

b. 主要的 IP 來源國家為美國、英國以及歐洲部分國家，紀錄上至少有 16 個國家。



F. 從封包行為來看，當主機收到外部 IP 的 UDP 封包後，會有大量的訊息回覆，回覆內容為重複的序列的字串。從往返封包大小可知，原本 60 bytes 的大小被放大至 1078 bytes，將近可達 18 倍，故可能導致對外頻寬壅塞。

No.	Time	Source	Destination	Protocol	Length	Info
1092	0.513725	24.241.248.144	140.[redacted].194	UDP	60	Source port: blackjack Destination port: chargen
1102	0.514948	140.[redacted].194	24.241.248.144	UDP	1078	Source port: chargen Destination port: blackjack
1146	0.535252	24.241.248.144	140.[redacted].194	UDP	60	Source port: blackjack Destination port: chargen
1156	0.536276	140.[redacted].194	24.241.248.144	UDP	1078	Source port: chargen Destination port: blackjack
1201	0.541820	24.241.248.144	140.[redacted].194	UDP	60	Source port: blackjack Destination port: chargen
1211	0.543287	140.[redacted].194	24.241.248.144	UDP	1078	Source port: chargen Destination port: blackjack

NetWitness Reconstruction for session ID: 21 (Source 190.213.165.75 : 1026, Target 140.[redacted].194 : 19)

Time 4/15/2014 14:36:27 to 4/15/2014 14:37:18 Packet Size 312,086 bytes Payload Size 289,761 bytes

Protocol 2048/17/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 442

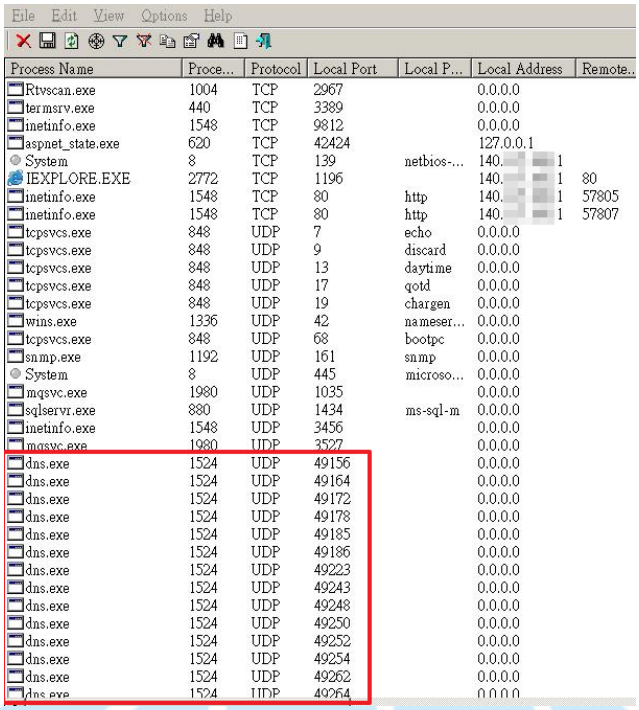
REQUEST

0

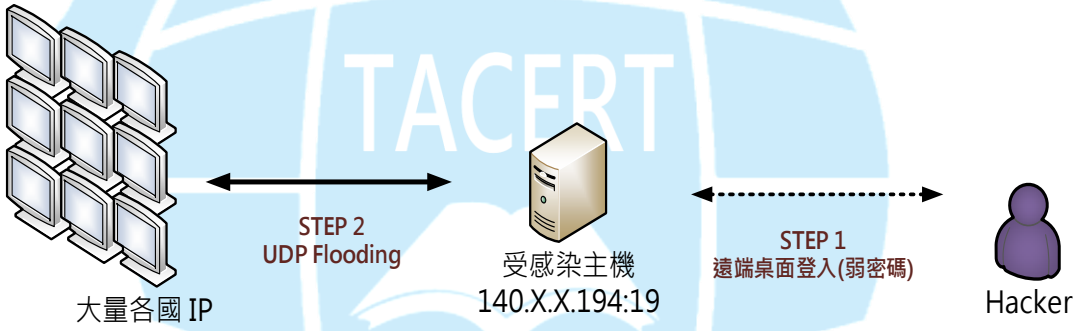
RESPONSE

```
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
/0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuv
0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvw
123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwx
23456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxy
3456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
```

G. 另外一種類似的網路行為是 DNS server 的服務，該程式 dns.exe 可能會被用來做為 DNS 放大攻擊。



三. 網路架構圖



STEP 1：主機遭受駭客遠端桌面入侵，利用windows內建的漏洞作為攻擊工具。

STEP 2：主機會開啟Port 19，並接收外部IP的封包後回覆大量封包形成UDP Flooding。

四. 建議措施

1. 手動將 tcpsvcs.exe 停用後移除，然而該檔案有可能會再次自動出現，原因可能是系統自動修復造成。

2. 建議直接從控制台的服務裡面，找到一個 DHCP server 的服

務，進入設定手動停用該服務，因為該服務會去呼叫 tcpsvcs.exe 啟用。

3. 管理者的密碼務必做變更，並且限制遠端桌面登入的來源端 IP。

4. 若是有大量 dns.exe 程序執行但不是正常使用 DNS 服務，則也能到控制台的服務設定，手動停用 DNS server 的服務，以避免被利用來作為 DNS 放大攻擊。

五. 總結

1. 此主機是因為有開放遠端桌面登入，然而沒有限制登入 IP 範圍，且管理者密碼長久未更改而被駭客破解。

2. 駭客登入後利用 windows server 的漏洞，利用內建的服務程式去做 UDP Flooding 的攻擊，成為駭客的工具跳板。

3. 因為 tcpsvcs.exe 和 dns.exe 是系統內建程式，防毒軟體並不會有偵測到木馬或病毒，但防毒軟體還是必須維持在較新的版本以防惡意程式植入。