

個案分析-

由 IRC Bot 引起的 ARP Spoofing

分析報告

TACERT

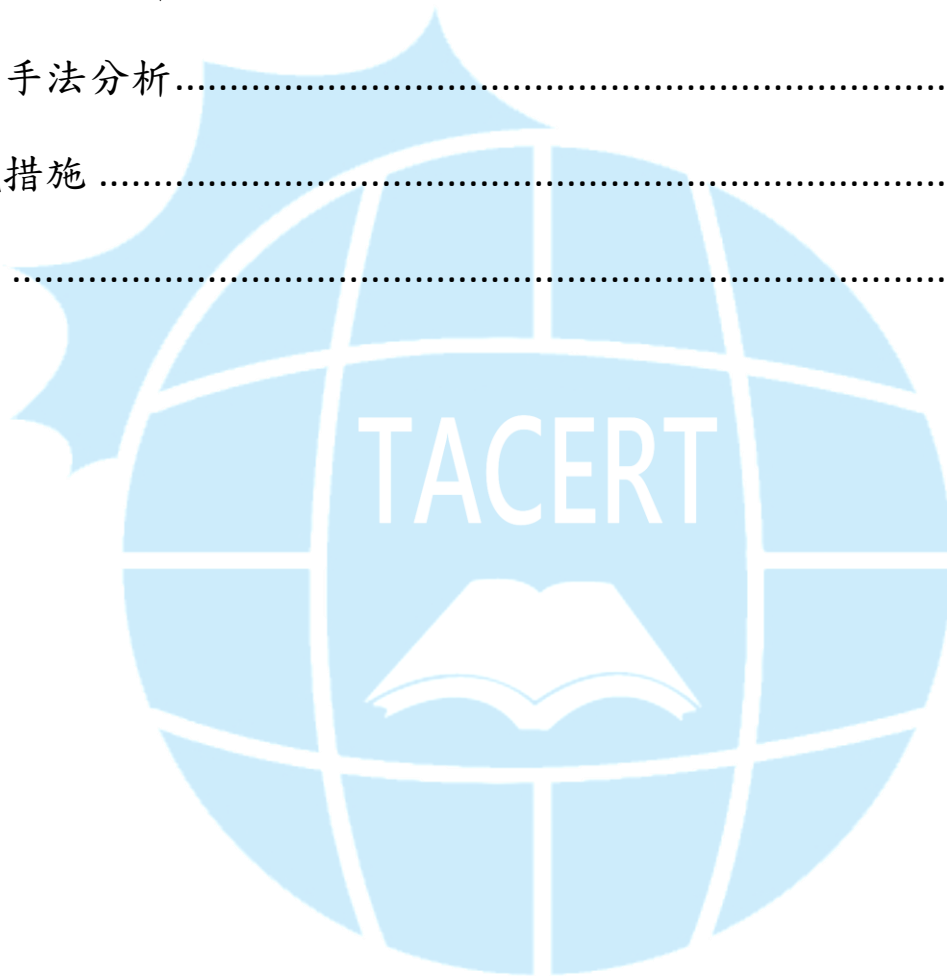
TACERT 臺灣學術網路危機處理中心團隊製

2012/4



目錄

事件說明	2
事件處理時間表.....	2
詳細流程	3
受駭主機分析.....	7
入侵手法分析.....	9
建議措施	9
參考	10





事件說明

一、事件發生時間：2012/3/17 至 2012/3/29

二、事件分類：區網內部 ARP SPOOFING

三、事件現象：2012/3/17 同區網內陸續傳出多台主機開機使用 DHCP 上網時，出現「IP 衝突」訊息，因而不斷地向 DHCP 主機要網路位址，然而 DHCP 主機可發派的位址已耗竭，許多使用 DHCP 上網的主機要不到 IP 無法上網。初步判斷有主機可能中了 ARP SPOOFING 病毒。調查具有「IP 衝突」主機後，發現並沒有異狀，轉而側錄該網段封包，發現封包中異常的 MAC 地址，循 MAC 地址找到導致此事件起因的主機。

事件處理時間表

表一、處理流程

時間	事件	說明
2012/03/20	對該區網內有「IP 衝突」而無法上網的電腦進行調查： <ul style="list-style-type: none"> ● 沒有掃描到惡意軟體 ● 該主機僅在使用 DHCP 上網會出現「IP 衝突」，使用 3G 等其他方法上網皆可正常使用 	判斷該主機並不是因為中毒才出現「IP 衝突」
2012/03/21	另外一台因為「IP 衝突」而被判可能中毒的電腦在重灌之後，仍持續有「IP 衝突」的問題，之後，使用固定位址上網解決了「IP 衝突」	判斷導致該區網多台電腦出現「IP 衝突」的原因並非主機本身
2012/03/22 2012/03/27	在出現「IP 衝突」的主機上側錄網路封包	發現 ARP Table 有一個 MAC 地址綁了多個同網段的位址，並發



		現異常的 ARP 封包
2012/03/29	由 MAC 找到該攻擊實體主機。取主機網路狀況與主機檔案	在主機中發現 IRC Bot 的相關檔案

詳細流程

2012/03/19 某一學校機構的 C1.X2.68.0/24 網段陸續傳出多台電腦出現「IP 衝突」，導致無法上網，疑似大批電腦中毒現象。C1.X2.68.0/24 網段使用 DHCP 取得 IP 位址，位於該網段的主機開機之後向 DHCP 要 IP 以及網路開道、DNS 等資訊，DHCP 會發派沒有主機使用的 IP 給發出 DHCP 請求的主機，03/19 出現許多主機不斷地向 DHCP 要 IP 的現象。

出現「IP 衝突」的電腦使用其他方法可正常上網，在其他網段使用 DHCP 上網也正常。另外有一台因為「IP 衝突」被判中毒的電腦重灌之後仍持續有「IP 衝突」的問題，顯示「IP 衝突」並不是本機端電腦中毒引起，加上在這些主機上面找不到任何可疑的病毒，所以判定可能是因為沒有更新而有未修補的漏洞。

進行更新之後，「IP 衝突」問題仍存在，既不是病毒引起，也不是未更新而有漏洞存在，所以將問題的起因排除這些出現「IP 衝突」的電腦，轉而尋找其他原因。2012/03/22 側錄一台有「IP 衝突」現象的主機封包（MAC 地址為 14:da:e9:57:98:26），於封包中發現如圖 1 所示現象，該主機不斷跟 DHCP 請求 IP，得到 IP 後又發現該 IP 已經有其他主機使用，所以又重新請求。

DHCP Discover：主機發出廣播封包詢問是否有 DHCP 主機存在

DHCP Request：主機回應 DHCP 的位址指派

DHCP Decline：主機發現 DHCP 發派的位址已有人使用，拒絕這個發派

Time	Source	Destination	Protocol	Info
012-03-22 15:42:23.633603	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x866c2c8c
012-03-22 15:42:23.641943	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x866c2c8c
012-03-22 15:42:24.103686	0.0.0.0	255.255.255.255	DHCP	DHCP Decline - Transaction ID 0x866c2c8c
012-03-22 15:42:34.119109	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x75983501
012-03-22 15:42:34.632218	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x75983501
012-03-22 15:42:35.111593	0.0.0.0	255.255.255.255	DHCP	DHCP Decline - Transaction ID 0x75983501
012-03-22 15:42:45.117063	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x6cca821e
012-03-22 15:42:45.637394	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x6cca821e
012-03-22 15:42:46.104882	0.0.0.0	255.255.255.255	DHCP	DHCP Decline - Transaction ID 0x6cca821e
012-03-22 15:42:56.114380	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xf877bc8b
012-03-22 15:42:56.634238	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xf877bc8b
012-03-22 15:42:57.113274	0.0.0.0	255.255.255.255	DHCP	DHCP Decline - Transaction ID 0xf877bc8b
012-03-22 15:43:07.128327	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xae8a3fb
012-03-22 15:43:07.635530	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xae8a3fb
012-03-22 15:43:08.109903	0.0.0.0	255.255.255.255	DHCP	DHCP Decline - Transaction ID 0xae8a3fb
012-03-22 15:43:18.126120	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xf3d35942
012-03-22 15:43:18.635719	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xf3d35942
012-03-22 15:43:19.109193	0.0.0.0	255.255.255.255	DHCP	DHCP Decline - Transaction ID 0xf3d35942
012-03-22 15:43:29.123233	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x4f95e654

Frame 37721: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
 Ethernet II, Src: 14:da:e9:57:98:26 (14:da:e9:57:98:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)

圖 1、MAC 為 14:da:e9:57:98:26 的主機不斷的向 DHCP 發出請求

之後在該主機的 ARP Table 發現某個 MAC 綁了多個同網段的位址。為了判斷這些網路位址是否真有主機使用，在同一個網段 (C1.X2.68.0/24) 使用 PING 指令測試，實體位址為 00-08-9b-ca-7b-98 的 IP 皆有主機回應，但是從其他網段 PING 這些 IP 卻沒有回應。

介面: C1.X2.68.63 --- 0xa

網際網路網址	實體位址	類型
C1.X2.68.1	00-08-9b-ca-7b-98	動態
C1.X2.68.16	00-22-68-64-0e-0d	動態
C1.X2.68.23	8c-64-22-b5-32-45	動態
C1.X2.68.28	00-01-6c-6b-a2-f6	動態
C1.X2.68.33	00-08-9b-ca-7b-98	動態
C1.X2.68.37	20-cf-30-07-bf-0f	動態
C1.X2.68.41	00-1f-c6-7c-e5-5c	動態
C1.X2.68.77	14-da-e9-57-98-8c	動態
C1.X2.68.90	00-08-9b-ca-7b-98	動態
C1.X2.68.96	00-08-9b-ca-7b-98	動態
C1.X2.68.97	00-0a-e4-f9-b5-f1	動態
C1.X2.68.110	8c-64-22-b5-32-45	動態
C1.X2.68.130	00-1e-33-24-4b-e0	動態
C1.X2.68.141	00-08-9b-ca-7b-98	動態
C1.X2.68.148	e8-e0-b7-32-7f-56	動態
C1.X2.68.153	00-08-9b-ca-7b-98	動態
C1.X2.68.164	54-04-a6-2e-f6-71	動態
C1.X2.68.167	00-08-9b-ca-7b-98	動態
C1.X2.68.173	00-08-9b-ca-7b-98	動態

C1.X2.68.179	00-08-9b-ca-7b-98	動態
C1.X2.68.187	00-08-9b-ca-7b-98	動態
C1.X2.68.190	00-01-6c-6b-a2-ee	動態
C1.X2.68.193	50-e5-49-50-3f-31	動態
C1.X2.68.200	00-1d-60-e3-fa-fa	動態
C1.X2.68.213	00-22-68-64-0d-fb	動態
C1.X2.68.254	f8-c0-01-ce-15-01	動態
C1.X2.68.255	ff-ff-ff-ff-ff-ff	靜態

表 1、C1.X2.68.0 網段某主機 ARP Table

同時也發現一個 MAC 為 00:08:9b:ca:7b:98 的主機，不斷地發出異常的 ARP 封包，詢問不再該網段內的主機，頻率約莫每一秒一次（如圖 2），其詢問的 IP 如表 2 所列。ARP Table 與異常的 ARP 封包都由同一個 MAC 產生，判斷該 MAC 為「IP 衝突」事件的起因，查出該主機為某實驗室擁有的 NAS 主機。

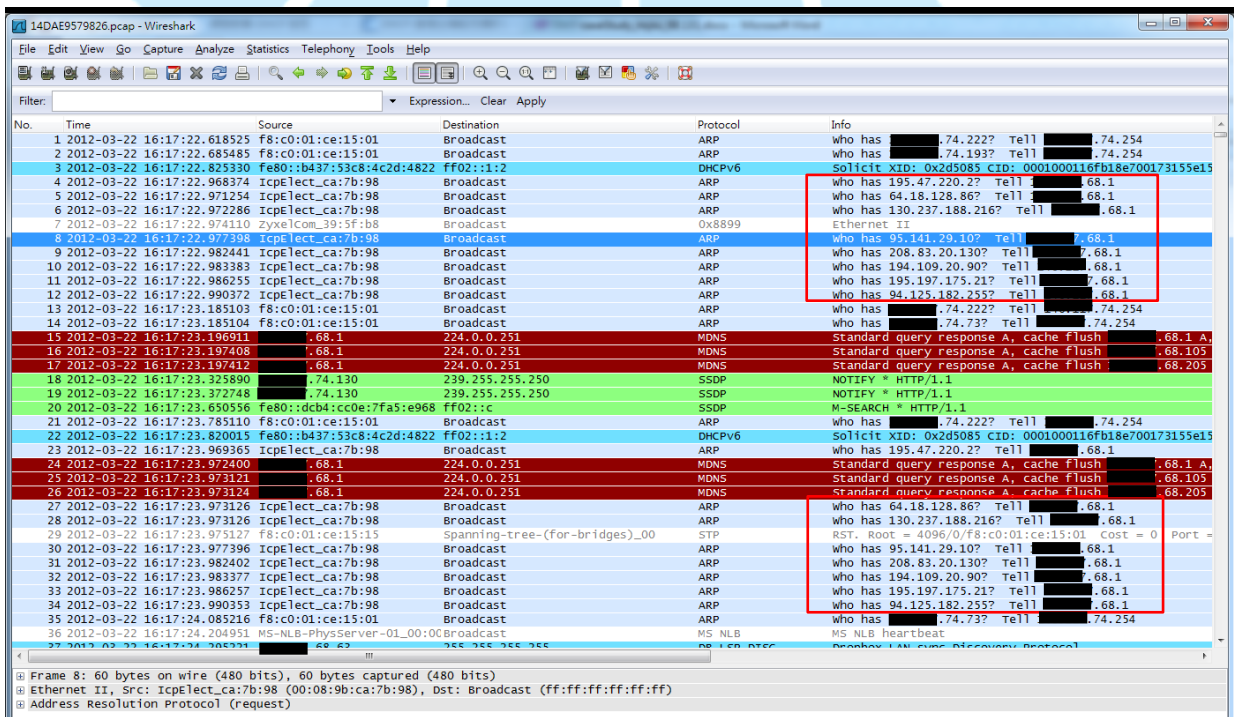


圖 2、異常的 ARP 封包

IP	Country	
95.141.29.10	德國	irc.euro-transit.net
208.83.20.130	美國	irc.undernet.org
194.109.20.90	荷蘭	irc.undernet.org



195.197.175.21	芬蘭	irc2.saunalahti.fi
94.125.182.255	匈牙利	irc.undernet.org
195.47.220.2	哈薩克	ircu.atw.hu
64.18.128.86	美國	irc.justedge.net
130.237.188.216	瑞典	irc.undernet.org

表 2、異常的 ARP 封包所詢問的 IP[1]



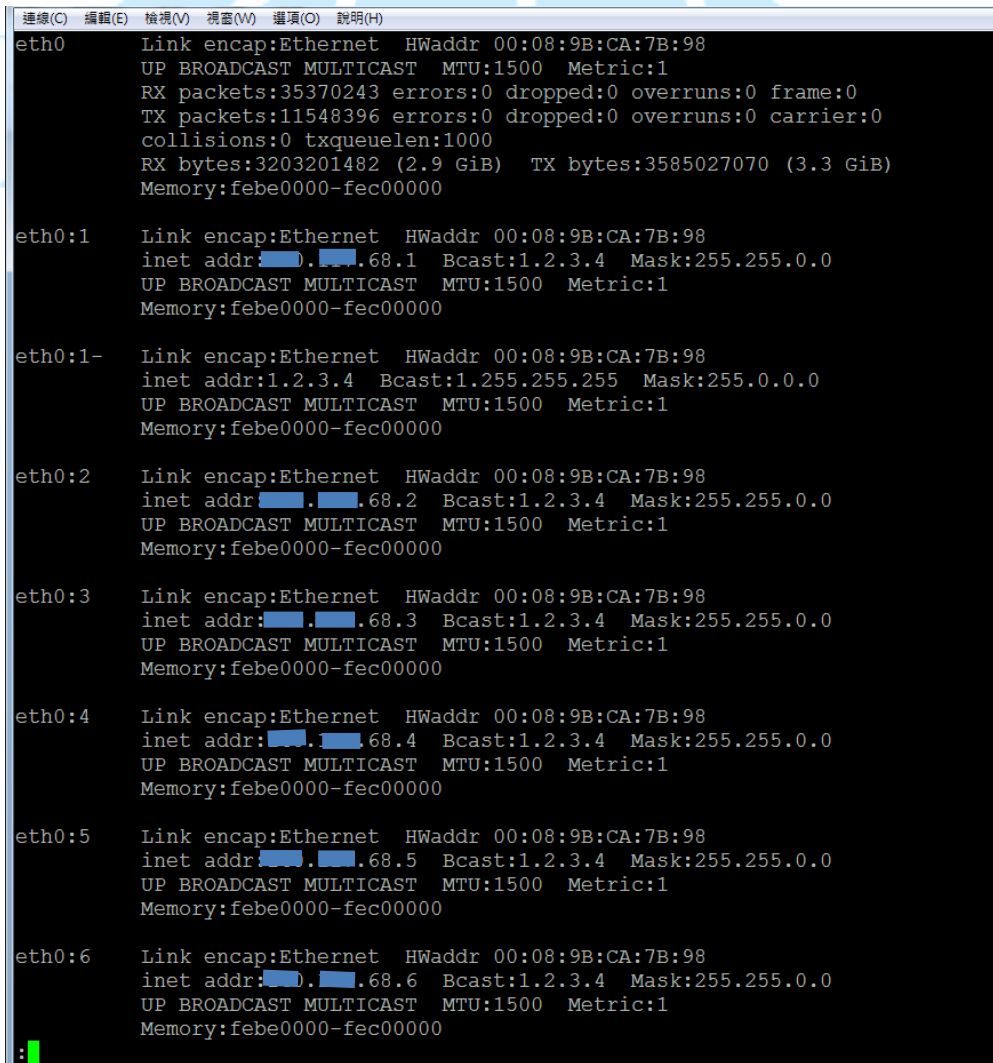
攻擊主機分析

MAC 地址為 00:08:9b:ca:7b:98 的主機資料：

硬體：QNAP TS-239 Pro II+

主機用途：提供資料儲存

許多主機出現「IP 衝突」的現象，是因為 MAC 地址為 00:08:9b:ca:7b:98 的主機沒有透過 DHCP 取得 IP，私自綁了該網段的許多 IP 在主機上，而 DHCP 並沒有這些 IP 被使用的紀錄，所以將 IP 發派出去後，客戶端會馬上出現「IP 衝突」。



```
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
eth0      Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:35370243 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11548396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3203201482 (2.9 GiB)  TX bytes:3585027070 (3.3 GiB)
          Memory:febe0000-fec00000

eth0:1    Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          inet addr:.....68.1 Bcast:1.2.3.4 Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Memory:febe0000-fec00000

eth0:1-   Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          inet addr:1.2.3.4 Bcast:1.255.255.255 Mask:255.0.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Memory:febe0000-fec00000

eth0:2    Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          inet addr:.....68.2 Bcast:1.2.3.4 Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Memory:febe0000-fec00000

eth0:3    Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          inet addr:.....68.3 Bcast:1.2.3.4 Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Memory:febe0000-fec00000

eth0:4    Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          inet addr:.....68.4 Bcast:1.2.3.4 Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Memory:febe0000-fec00000

eth0:5    Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          inet addr:.....68.5 Bcast:1.2.3.4 Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Memory:febe0000-fec00000

eth0:6    Link encap:Ethernet  HWaddr 00:08:9B:CA:7B:98
          inet addr:.....68.6 Bcast:1.2.3.4 Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Memory:febe0000-fec00000
```

圖 3、MAC 為 00:08:9b:ca:7b:98 的主機綁了許多個 IP

在隱藏目錄/mnt/hda_root/.config/ssh/ecmf/.x 下有駭客入侵後下載的檔案，圖 4 列出主要的幾個檔案，圖五為 m.set 檔內容，由這些檔案內容可以推斷駭客意圖在主機植入 IRC Bot，但由於主程式 xh，由 perl 寫成，而受害主機上並沒有安裝 perl，且網路流量也沒有發現與 IRC 有關的流量，故推斷受害主機上的 IRC Bot 並沒有執行成功。駭客僅在網路狀態設定上有成功，至於在該主機上綁了許多 IP，應是為了使主機在大量 IP 的掩護下連上 IRC Server，躲避偵測。

```
68.93.user2: ASCII text
68.95.user: ASCII text
68.95.user2: ASCII text
68.96.user: ASCII text
68.96.user2: ASCII text
68.98.user: ASCII text
68.98.user2: ASCII text
68.99.user: ASCII text
68.99.user2: ASCII text
68.9.user: ASCII text
68.9.user2: ASCII text
autorun: POSIX shell script text executable
cron.d: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (u
ses shared libs), for GNU/Linux 2.2.5, not stripped
cron.d: ASCII text
inst: POSIX shell script text executable
LinkEvents: ASCII text
mech.dir: ASCII text
m.help: data
m.lev: ASCII text
m.pid: ASCII text
m.ses: ASCII C++ program text
m.set: ASCII text
r: directory
run: POSIX shell script text executable
start: POSIX shell script text executable
update: POSIX shell script text executable
vhosts: ASCII text
xh: a /usr/bin/perl script text executable 主程式
```

圖 4、隱藏目錄/mnt/hda_root/.config/ssh/ecmf/.x 下的檔案

```
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
SERVER 208.83.20.130 6667
SERVER 208.83.20.130 6668
SERVER 208.83.20.130 7000
SERVER 95.141.29.10 6660
SERVER 95.141.29.10 6669
SERVER 95.141.29.10 7000
SERVER 195.197.175.21 6660
SERVER 195.197.175.21 6669
SERVER 195.197.175.21 7000
SERVER 194.109.20.90 6660
SERVER 194.109.20.90 6669
SERVER 194.109.20.90 7000
SERVER 194.109.20.90 9000
SERVER 94.125.182.255 6660
SERVER 94.125.182.255 6667
SERVER 64.18.128.86 6661
SERVER 64.18.128.86 7000
SERVER 130.237.188.216 6667
SERVER 130.237.188.216 6669
SERVER 195.47.220.2 6667
SERVER 195.47.220.2 6669
```

圖 5、m.set 檔裡的内容與異常 ARP 封包所詢問的 IP 符合



入侵手法分析

- 主機使用簡單帳號密碼 (admin/admin)
- 主機使用出廠預設帳號密碼 (admin/admin)
- 未限制最大權限管理者遠端登入的位址

由於 QNAP 公司的 NAS 出廠之後的管理者帳號和密碼預設都是 admin/admin，為一組經典的簡單帳號與密碼，該台主機管理者並沒有改變其密碼，也沒有限制遠端登入的位址，加上該主機命令列的 History 最後是刪除命令列的歷史紀錄，所以確定駭客使用 SSH 登入取得主機控制權進行入侵。

建議措施

區網管理者

- 使用 DHCP 上網的網段，建議無 DHCP 紀錄的 IP 應禁止其對外連線
- 網域開道的 ARP TABLE 可參照 DHCP 的 IP 租用紀錄靜態設置

一般使用者

- 更改管理員密碼，不使用字典詞彙
- 不使用出廠預設密碼
- 對 super user 的遠端登入進行控管



參考

- [1] Robtex Swiss Army Knife Internet Tool, <http://www.robtex.com/>

