個案分析-

對外進行 RDP 攻擊的主機事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2016/12

I. 事件簡介

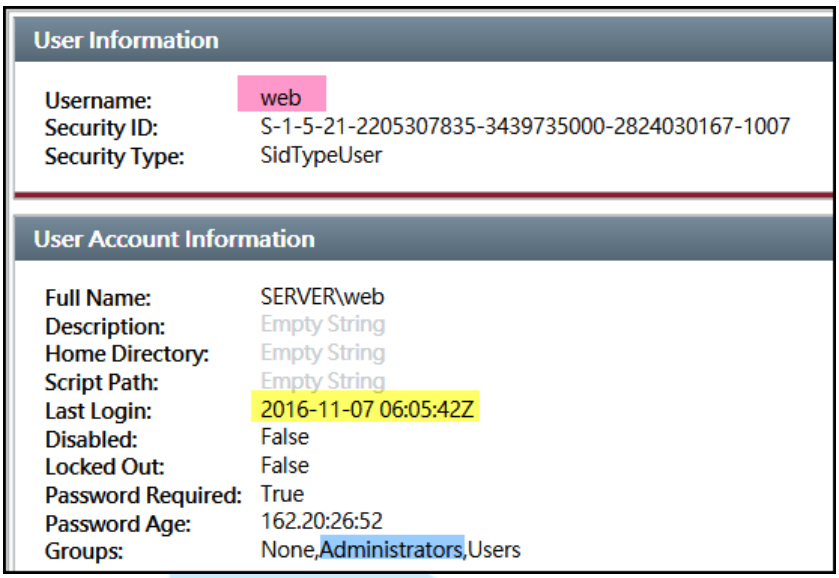
1. 近期接獲其他單位情資顯示,該校主機疑似有中繼站或 C&C 的連線特徵。
2. 與該主機管理者聯繫後，同意讓本單位前往進行數位鑑識及惡意流向側錄。
3. 該主機為某系所的伺服器，並且使用系統 Windows Server 2003，為 Web Server。
4. 伺服器有啟用遠端桌面連線服務，讓管理者進行遠端管理，但並未限制連線來源端網段。

II. 事件檢測

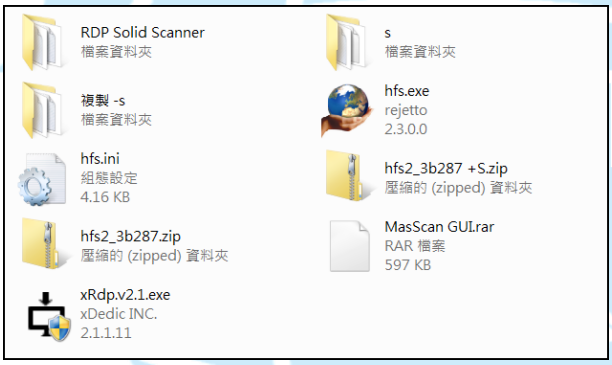
1. 首先使用 TCPView 查看主機的網路通訊狀態，得知目前有哪些服務是正在啟用為 Listening 或 Established,明顯看出主要為 Web 和 RDP service 正在啟用中，分別為 TCP port 80 和 3389。

Process	PID	Protocol	Local Address	Local Port	Remote Ad...	Remote P...	State	Sent Pa
[System Process]	0	TCP	140	80	115.82.9.174	61088	TIME_WAIT	
System	4	TCP	140	80	23.247.72.4	35993	ESTABLIS...	
System	4	TCP	0.0.0.0	80	0.0.0.0	0	LISTENING	
svchost.exe	736	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING	
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING	
lsass.exe	456	TCP	0.0.0.0	1025	0.0.0.0	0	LISTENING	
svchost.exe	2164	TCP	0.0.0.0	3389	0.0.0.0	0	LISTENING	
System	4	TCP	140	139	0.0.0.0	0	LISTENING	
System	4	UDP	0.0.0.0	445	*	*		
lsass.exe	456	UDP	0.0.0.0	500	*	*		
spoolsv.exe	1252	UDP	0.0.0.0	1026	*	*		
lsass.exe	456	UDP	0.0.0.0	4500	*	*		
svchost.exe	844	UDP	127.0.0.1	123	*	*		
svchost.exe	844	UDP	127.0.0.1	4527	*	*		
svchost.exe	844	UDP	140	123	*	*		
System	4	UDP	140	137	*	*		
System	4	UDP	140	138	*	*		

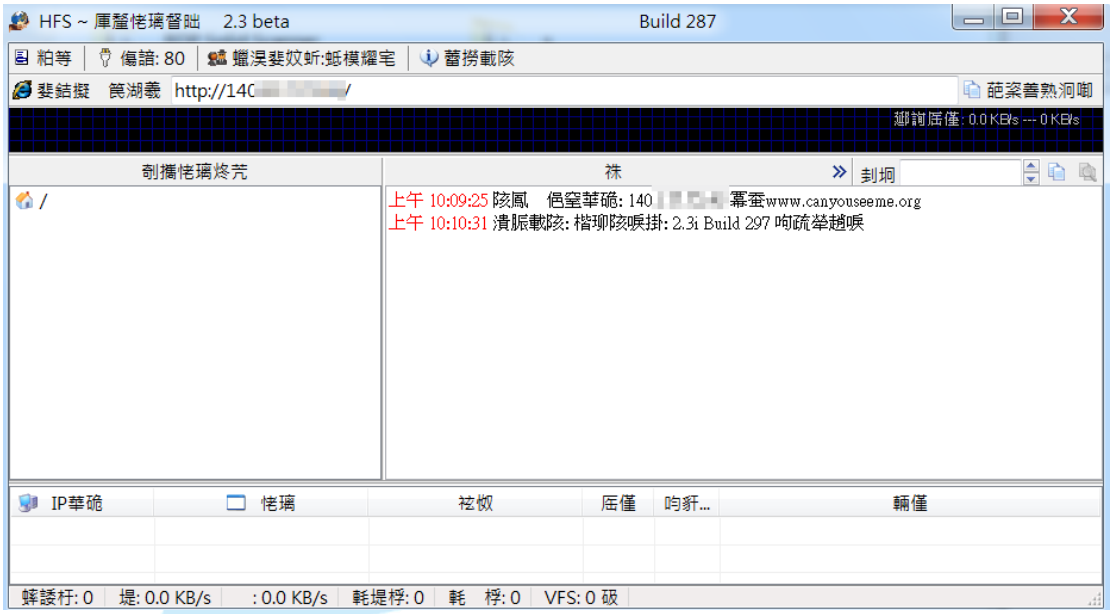
2. 檢查主機內帳號狀態除了 administrator 外，也有其他使用者帳號，其中帳號“web”顯示的活動紀錄最為明顯，且隸屬管理者群組帳號。



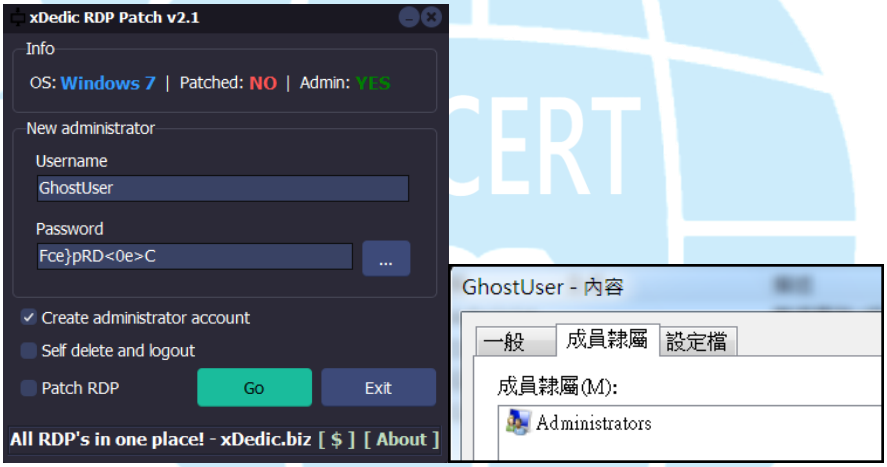
3. 檢查帳號 web 的家目錄中發現到許多的駭客遺留的工具檔案，包含許多文件檔和批次檔及執行檔，詳細檢查駭客的工具檔案發現，主要分為 IP、Port 掃描工具以及 RDP 帳號管理工具及檔案傳輸工具。



4. 以 hfs.exe 為例，該程式執行能夠快速創立 HTTP server，不用安裝直接執行，讓外部能夠透過 HTTP browser 存取伺服器內的資料，方便性上優於 FTP 傳輸。



5. 其次 xRdp.v2.1.exe 為用來建立主機帳號工具，能夠讓駭客快速建立管理者幽靈帳號及密碼，並且也能夠快速將帳號移除之。



6. 在資料夾“s”或“複製 -s”中，含有許多 IP 列表的文件檔，以及 s.exe 執行檔和批次檔。其中批次檔內容中可看到駭客所執行的 script 指令，能夠對特定 port 和 ip 進行掃描並將結果存入文件中。

3389.bat - 記事本

```
@echo off
setlocal
cls
color 2E
title SYN(syn)
for /f "eol= tokens=1,2 delims= " %%i in (ip.txt) do s syn %%i %%j 3367,3368,3370,3371,3376,3377,3378,
for /f "tokens=1,2,3" %%a in ('type result.txt') do (
  if "%%c"=="Open" (
    if not defined flag (
      set flag=a
      >result.txt echo %%a:%%b ) else (
      >>result.txt echo %%a:%%b
    )
  )
)

for /f "eol=- tokens=1 delims= " %%i in (result.txt) do echo %%i>>ips.txt

exit
```

7. 調查 ip.txt 內容為欲掃描的 IP 列表，而 s 為掃描程式 s.exe，result.txt 和 ips.txt 為掃描有開啟 port 的結果。然而在掃瞄 IP 列表中 TANET 的 IP 網段是被排除的，推測可能規避偵測設備。

ips.txt - 記事本

```
125.141 141:3387
125.141 143:3378
125.141 142:3368
125.141 140:3382
125.141 141:3393
125.141 141:3390
125.141 143:33881
125.141 142:3382
125.141 143:9833
125.141 143:3387
125.141 143:3396
125.141 140:3376
```

Result.txt - 記事本

```
210.112 216:3390
210.112 216:33980
210.112 218:3376
210.112 216:3380
210.112 216:3382
210.112 216:3384
210.112 216:3398
210.112 216:3381
210.112 216:33890
210.112 218:3378
210.112 218:3386
210.112 216:3385
```

8. 檢查後發現到有一文件檔 tw3-9.txt 中，包含所有台灣網段以及 TANET 網段掃描結果，應該是駭客另外針對台灣進行掃描歸檔。

tw3-9.txt - 記事本

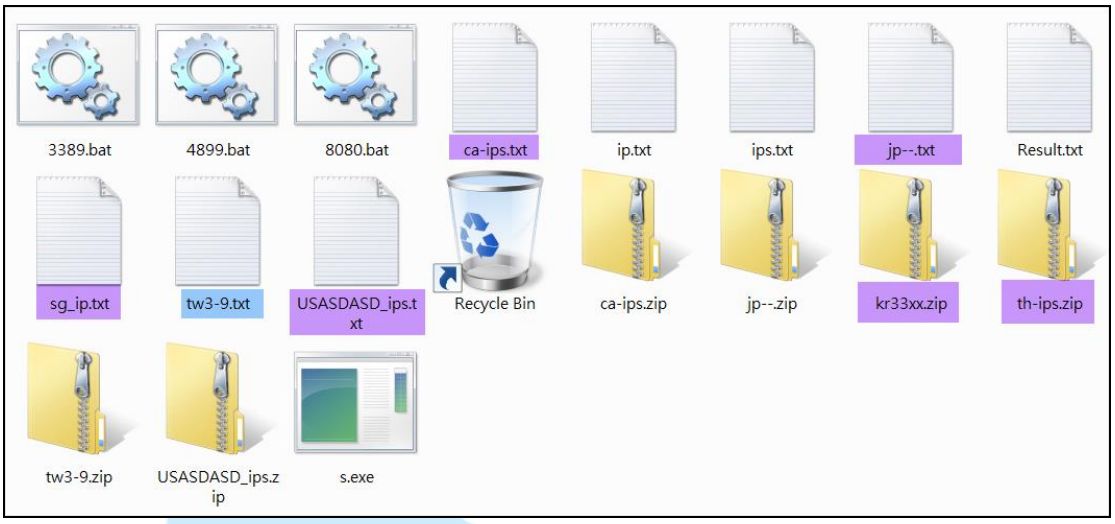
```
140. 8.247:33880
140. 8.248:3399
140. 8.247:33990
140. 8.248:3389
140. 8.247:3388
140. 8.249:33890
140. 8.249:33990
140. 8.248:3390
140. 8.250:3389
140. 8.249:3388
140. 8.248:3387
140. 8.250:33990
140. 8.248:33880
140. 8.249:3390
```

tw3-9.txt - 記事本

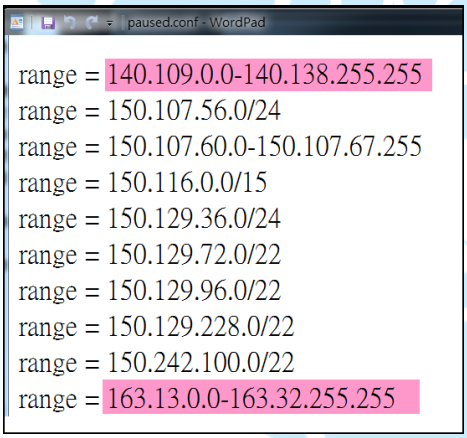
```
163. 92.175:3390
163. 92.175:33990
163. 92.176:3390
163. 92.176:33990
163. 92.177:33990
163. 92.177:3390
163. 92.178:33990
163. 92.178:3390
163. 92.179:3390
163. 92.191:33990
163. 92.192:33990
163. 92.192:3390
163. 92.193:33990
163. 92.193:3390
```

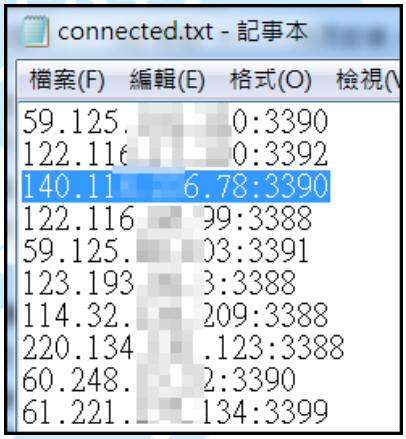
9. 除了台灣網段之外，駭客還掃描了其他國家分類存檔，包含加拿大、美國、

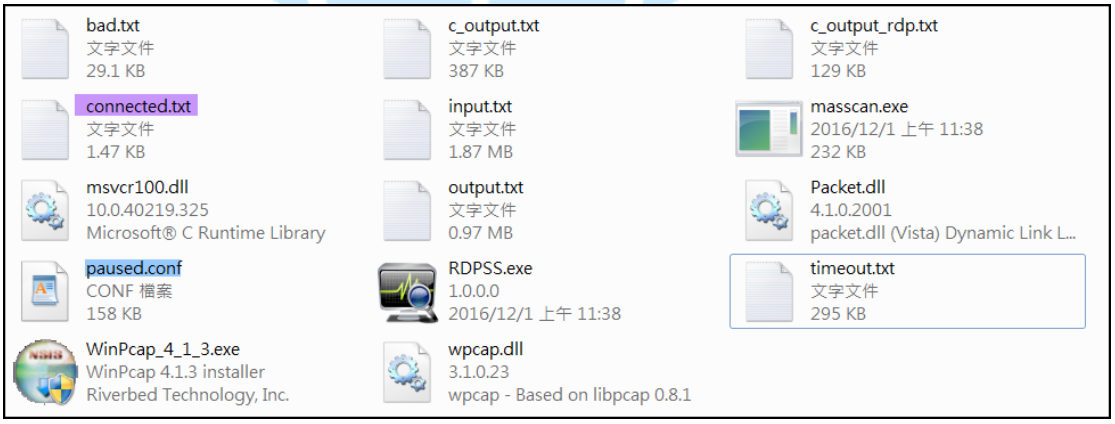
新加坡、泰國、日本、韓國。



10.除了 s.exe 之外，駭客還使用 RDP Solid Scanner 的工具進行 RDP 服務的掃瞄，值得注意的是該工具的設定中 pause.conf 可以看到有明確指定 TANET 網段範圍，並且將疑似成功破解連入的 IP 寫入檔案 connected.txt 中，其中有一筆 140.11X.X.X 為 TANET IP。

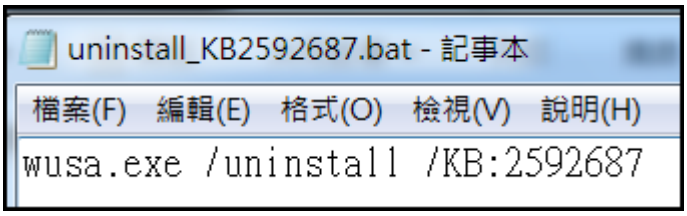




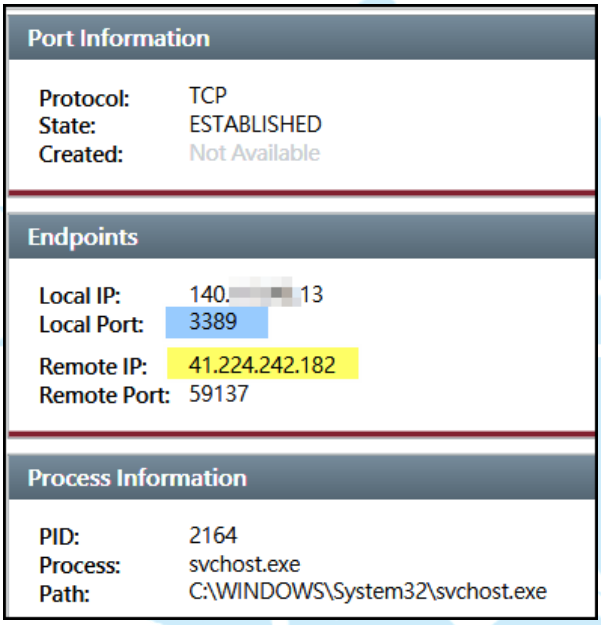


11.在使用 RDPSS 掃埠工具之前，駭客會先移除 KB2592687 的 RDP 漏洞修

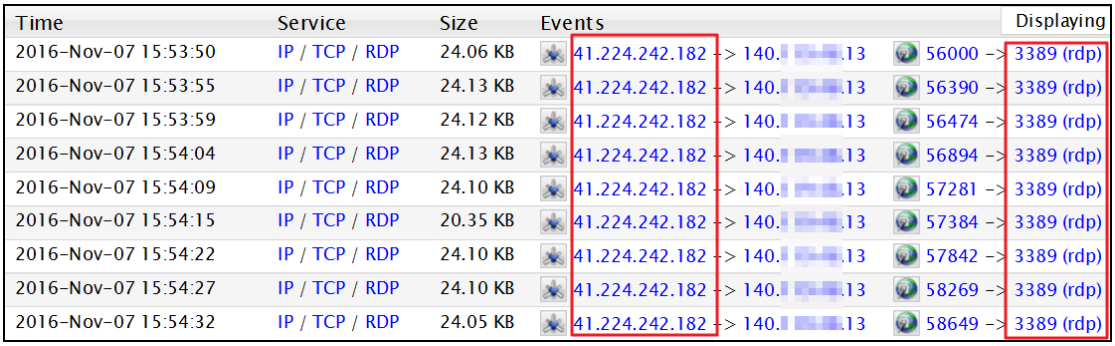
補，以確保 RDP scan 能夠順利進行。



12. 檢查記憶體中紀錄的連線狀態，確實剛好有 port 3389 的連線被建立，表示有人正在嘗試遠端桌面連線登入主機。此連線 IP 為 41.224.242.182，為位於北非的突尼西亞國家。



13. 檢視側錄封包的 RDP 連線資訊，IP 41.224.242.182 持續密集對主機發送 RDP 的連線封包，封包大小都只有 20 多 KB，推測正在進行 RDP 的暴力破解攻擊。



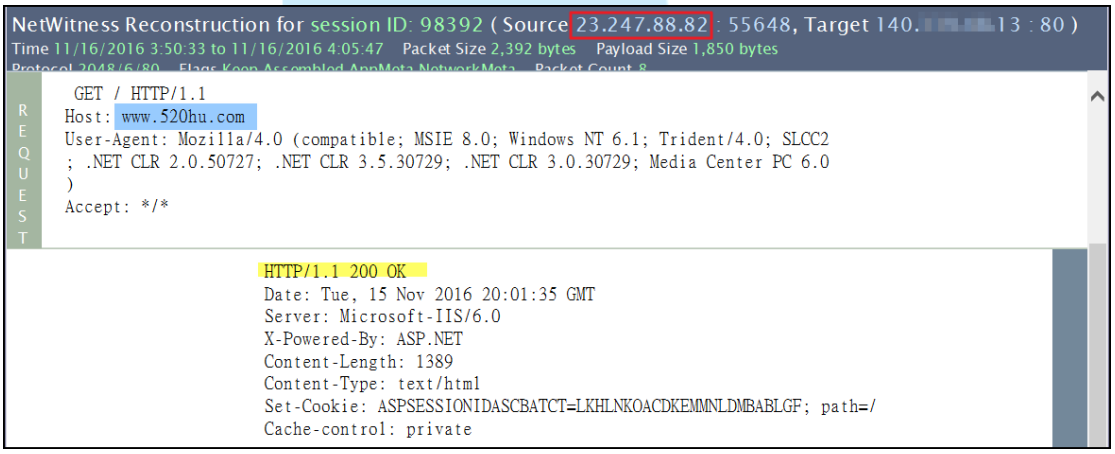
Time	Service	Size	Events	Displaying
2016-Nov-07 15:53:50	IP / TCP / RDP	24.06 KB	41.224.242.182 -> 140. .13	56000 -> 3389 (rdp)
2016-Nov-07 15:53:55	IP / TCP / RDP	24.13 KB	41.224.242.182 -> 140. .13	56390 -> 3389 (rdp)
2016-Nov-07 15:53:59	IP / TCP / RDP	24.12 KB	41.224.242.182 -> 140. .13	56474 -> 3389 (rdp)
2016-Nov-07 15:54:04	IP / TCP / RDP	24.13 KB	41.224.242.182 -> 140. .13	56894 -> 3389 (rdp)
2016-Nov-07 15:54:09	IP / TCP / RDP	24.10 KB	41.224.242.182 -> 140. .13	57281 -> 3389 (rdp)
2016-Nov-07 15:54:15	IP / TCP / RDP	20.35 KB	41.224.242.182 -> 140. .13	57384 -> 3389 (rdp)
2016-Nov-07 15:54:22	IP / TCP / RDP	24.10 KB	41.224.242.182 -> 140. .13	57842 -> 3389 (rdp)
2016-Nov-07 15:54:27	IP / TCP / RDP	24.10 KB	41.224.242.182 -> 140. .13	58269 -> 3389 (rdp)
2016-Nov-07 15:54:32	IP / TCP / RDP	24.05 KB	41.224.242.182 -> 140. .13	58649 -> 3389 (rdp)

14. 檢視其中一筆封包內容，可以看到有人正在嘗試用帳號 manager 登入失

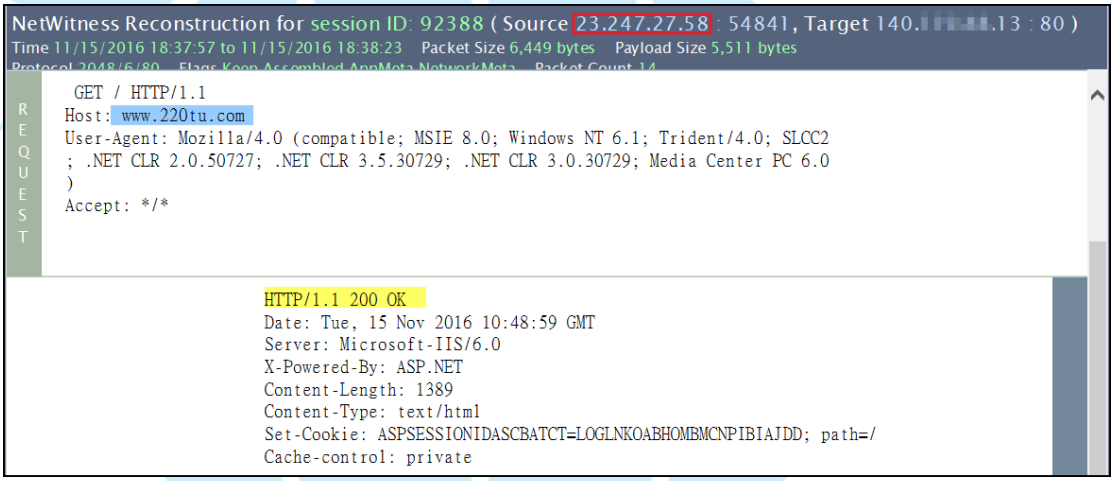
敗，並且會持續使用不同帳號進行暴力破解登入。

15. 檢查封包紀錄發現疑似中繼站的連線行為，雖然此主機目前沒有明確的中繼站連線，但是有許多外部 IP 會透過網域名稱嘗試存取 port 80，而這些網域名稱有成人網站或大陸網站的位址。

16. 此連線紀錄 IP 23.247.88.82 嘗試透過網址 www.520hu.com 連線，而該網址當時剛好解析出來的 IP 之一為該主機，此網址會轉跳至成人網站入口網頁 www.bu577.com 。

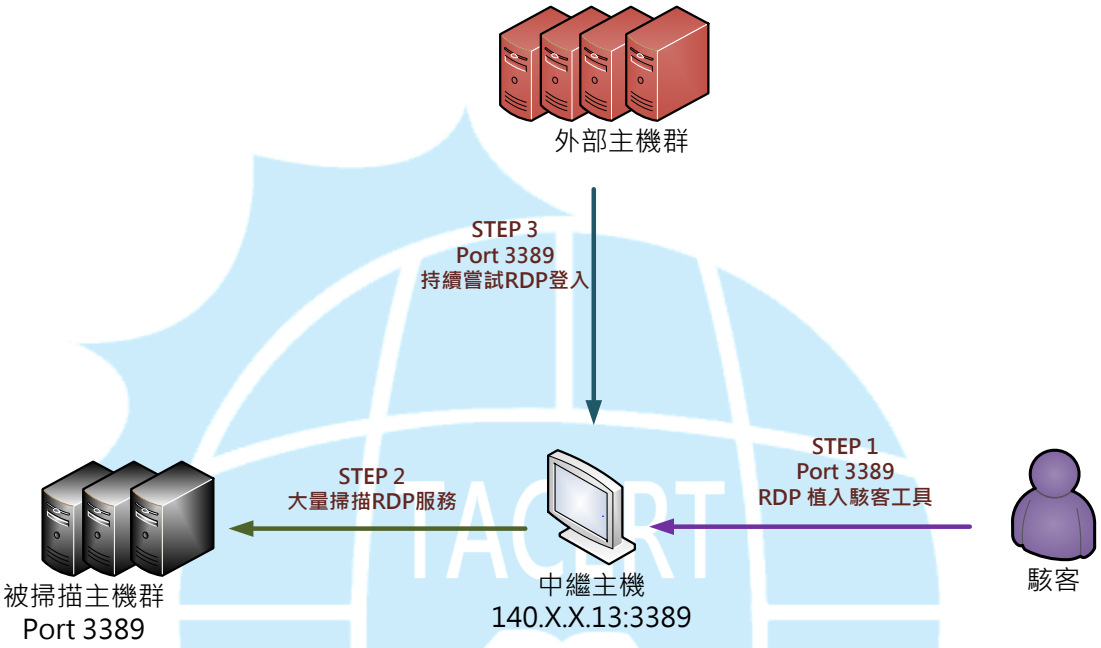


17. 此連線紀錄 IP 23.247.27.58 嘗試透過網址 www.220tu.com 連線，而該網址當時剛好解析出來的 IP 之一為該主機，此網址也會轉跳至成人網站入口網頁 www.bu660.com。



18. 由於該主機在鑑識之前有重新開機過，因此擷取的記憶體中並無重開機之前的程式連線紀錄。駭客似乎也察覺到行蹤被發現，故封包側錄過程中並無再次登入的跡象。

III. 網路架構圖



1. 駭客透過遠端桌面服務成功登入 web 帳號，並植入駭客工具。
2. 駭客利用中繼主機對外大量掃描 port 3389 或可能的 RDP 服務。
3. 同時外部大量主機也會不斷地嘗試入侵遠端桌面服務 RDP。
4. 駭客除了利用主機做 RDP 掃描，也可能會用來發動 DDoS 攻擊或中繼資料。

IV. 建議與總結

1. 該主機為系所的網站伺服器，並且有開啟遠端桌面 RDP 服務讓管理者登入。
2. 當初伺服器架設時候有創立一個 Web 帳號，管理者並不清楚該帳號使用狀態。
3. 該主機並無設定防火牆規則限制 RDP 連入網段，導致 web 帳號被暴力破

解入侵。

4. 由於 Web 帳號屬於 administrator 群組，因此在權限上可以安裝執行任何程式，而該主機的師生資料也可能早已外洩。
5. 建議管理者定期清查主機所有帳號使用狀態，並設定群組權限。
6. 建議將 RDP 遠端桌面服務增設 ACL 規則，避免外部不明人士暴力破解登入。
7. 建議定期檢查網路連線狀態及背景是否有可疑連線程式，並安裝防毒軟體防護。