

TACERT 資安電子季報 - 第二季

目錄：

最新消息	1
本季資安事件類型趨勢	2
安全性公告	2
個案分析-Y 大學大量對外進行 SSH 攻擊主機事件分析報告	3
個案分析-P 大學遭植入惡意後門程式的主機事件分析報告	5
資安新知-SSDP 及 UPnP 漏洞攻擊	7
TACERT 組織介紹	7

TACERT 資安電子季報簡介

TACERT 資安電子季報由臺灣學術網路危機處理中心(TANet Computer Emergency Response Team, 簡稱 TACERT)中心負責編撰，自 2012 年度起，每季將匯整當季學術網路資安事件類型趨勢、安全性公告、資安事件個案分析、資安新知等資訊，期能提供學術網路使用者學習資安知識與能力，共同加強學術網路的防護。

最新消息

- ◆ 臺灣學術網路危機處理中心為加強臺灣學術網路(TANet)網路安全防護能力，於 7~8 月份辦理三場次的「開源碼網站安全暨防護實作之資安巡迴研討會」，本次研討會重點在於推廣使用開放原始碼 (Open Source)來強化校園的網路安全防護能力。研討會詳細資訊請參閱：<http://tacert.mis.nsysu.edu.tw>。

資安網站連結

- * [TACERT 網站](#)
- * [教育機構資安通報平台](#)
- * [教育部全民資安素養網](#)

近期資安活動

- ◆ 2015/5/28-2015/5/29 [第二十五屆全國資訊安全會議](#)
- ◆ 2015/7~2015/8 [開源碼網站安全暨防護實作之資安巡迴研討會](#)



本季資安事件類型趨勢

教育機構資安通報平台自 104 年 4 月至 6 月，共成立 4,678 張資安事件單資安事件類型大致可分為 INT (Intrusion, 入侵攻擊) 與 DEF (Deface, 網頁攻擊) 兩種類型。本季 INT 類型佔所有資安事件類型中的 98%，其 INT 類型(圖 2)又以「系統被入侵」、「對外攻擊」及「殭屍網路 BOT」的子類型比率最高，觀察本季學術網路資安事件有較下降的趨勢。

DEF 類型(圖 3)以「惡意網頁」、「網頁置換」及「釣魚網站」的子類型佔前三名。目前只要於 TANet 中偵測到有釣魚網站、嚴重的 mail spam 或其他嚴重影響網路資源的資安事件發生，教育部資訊及科技教育司會先進行封鎖作業，以避免造成更大之危害，待受害單位完成資安事件通報應變處理後，並通過教育部資訊及科技教育司的複審確認已無安全性風險，才可解除限制。有關 TANet ANTI-SPAM 網址：<http://rs.edu.tw/tanet/spam.html>。

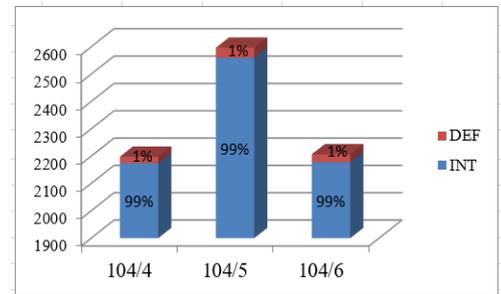


圖 1. 104 年第二季資安事件類型比例圖

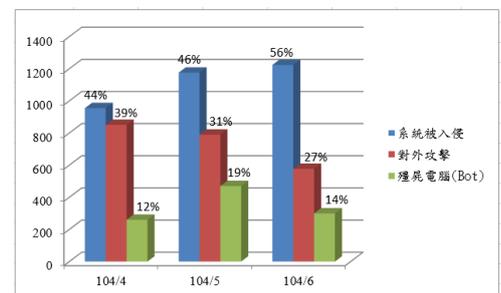


圖 2. 104 年第二季 INT 子類型前三名比例圖

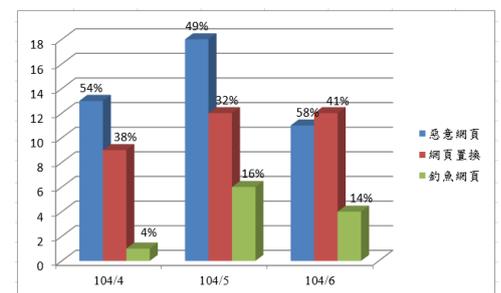


圖 3. 104 年第二季 DEF 子類型前三名比例圖

安全性公告

- ※ [104/04/14 微軟 4 月份發佈 11 項安全公告，請儘速更新。](#)
- ※ [104/04/14 Apple OS X、iOS、Safari、Apple TV 存在多重弱點，建請更新！](#)
- ※ [104/04/24 HTTP.sys 中的資訊安全風險可能會允許遠端執行程式碼，建請更新！](#)
- ※ [104/05/12 微軟 5 月份發佈 13 項安全公告，請儘速更新。](#)
- ※ [104/05/22 Cisco UCS Central Software 存在安全弱點，建議請管理者評估更新！](#)
- ※ [104/06/09 微軟 6 月份發佈 8 項安全公告，請儘速更新。](#)
- ※ [104/06/11 SSL/TLS 加密協定存在中間人攻擊破解加密金鑰弱點，建請盡快修正！](#)
- ※ [104/06/11 微軟 Kerberos 弱點被利用，可導致允許權限提高，建議立即進行安全性更新！](#)



資安事件個案分析-Y 大學大量對外進行 SSH 攻擊的主機事件分析報告-1

※ 事件簡介：

- 一. 該校被偵測單位偵測到有大量對外攻擊行為，並開立資安事件單。該校的主機管理者請本單位協助解決，並且進行主機的數位鑑識。
- 二. 經詢問該主機為一台 Ubuntu Linux 的作業系統，並且有架設 Centos 虛擬機提供對外學生的遠端桌面服務。上層的 Centos 虛擬機透過 NAT 方式與底層 Ubuntu 共用對外實體 IP，故必須同時對兩個作業系統進行檢測。
- 三. 該主機檢測前已先斷開網路線，本單位安裝網路分歧器進行封包側錄後才恢復網路。

※ 事件檢測

- 一. 恢復網路後進入底層主機 terminal 介面，透過 netstat 指令先觀察是否有可疑的網路連線。因管理者告知該主機有重新啟動過，故一開始並無發現可疑連線。
- 二. 該主機有啟用 port 21、22、3389 的服務，分別為 FTP、SSH 及 RDP 服務讓管理者能夠登入使用，因此猜測駭客可能透過這些服務漏洞入侵。
- 三. 檢查 Ubuntu 的登入記錄檔 auth.log(如圖 4 所示)確實發現到資安事件單派發日期前有可疑的 IP 登入紀錄。帳號 test 分別有兩筆紀錄在 22 號以前成功以 SSH 方式登入主機，IP 分別是中國的 119.147.144.101 和香港的 59.188.237.12。
- 四. 檢查主機內是否有可疑的檔案或自動執行排程(如圖 5 所示)，結果相當乾淨找不出有問題檔案。故研判應為駭客一次性入侵執行程式，一旦程式被關閉則不留痕跡。將主機閒置一段時間並觀察是否會再次被入侵，果然發現帳號 test 有再次被登入的紀錄 59.188.237.12 為上次相同登入的香港 IP，並且記錄中有使用 sftp 協定植入後門程式，確定為駭客故意入侵行為。
- 五. 主機管理者告知說 test 初始是替廠商創立維護使用。但隨後維護結束後已透過指令 userdel 將帳號疑除，實地檢查帳號 test 的家目錄的確已被移除。然而檢查 /etc/passwd 帳號管理檔案卻能發現 test 依然存在，實地測試依舊能夠透過 SSH 登入，只是沒有家目錄存在。該 test 帳號能夠輕易被入侵主要原因之一是使用 test1234 的弱密碼。
- 六. 此時 netstat 檢查網路連線狀態，確實出現了大量的對外連線(如圖 6 所示)，都是連到外部 IP 的 port 22，也就是正在進行 SSH 的暴力破解攻擊。檢查網路使用資源幾乎是耗盡所用頻寬，故導致系統效能降低以及其他人網路變慢。

```
root@ubuntu:~# less /var/log/auth.log | grep Accepted
Apr 20 10:46:07 ubuntu sshd[3703]: Accepted password for test from 119.147.144.101 port 57956 ssh2
Apr 20 14:27:46 ubuntu sshd[20930]: Accepted password for test from 59.188.237.12 port 1508 ssh2
Apr 22 00:13:46 ubuntu sshd[32213]: Accepted password for test from 59.188.237.12 port 4899 ssh2
Apr 23 22:31:15 ubuntu sshd[9673]: Accepted password for test from 36.238.142.236 port 9162 ssh2
root@ubuntu:~#
```

圖 4.

```
root@ubuntu:~# less /var/log/auth.log | grep Accepted
Apr 27 16:38:18 ubuntu sshd[32742]: Accepted password for test from 140. port 62083 ssh2
Apr 27 16:41:39 ubuntu sshd[909]: Accepted password for test from 140. port 19161 ssh2
Apr 27 16:44:45 ubuntu sshd[1426]: Accepted password for test from 140. port 51318 ssh2
Apr 27 16:58:42 ubuntu sshd[3595]: Accepted password for test from 140. port 19857 ssh2
Apr 27 17:37:08 ubuntu sshd[3609]: Accepted password for test from 59.188.237.12 port 1971 ssh2
root@ubuntu:~#
```

圖 5.

```
tcp 0 1 140. 161.33501 200.14.56.140:22 SWN_SENT 1000/squid64
tcp 0 1 140. 161.60903 157.201.144.87:22 SWN_SENT 9392/squid64
tcp 0 296 140. 161.59055 78.188.113.17:22 ESTABLISHED 10610/squid64
tcp 0 1 140. 161.84624 159.79.52.13:22 SWN_SENT 9188/squid64
tcp 0 1 140. 161.33495 65.179.173.230:22 SWN_SENT 1000/squid64
tcp 0 0 140. 161.58810 113.88.241.22:22 ESTABLISHED -
tcp 0 0 140. 161.53531 69.46.19.48:22 ESTABLISHED 8781/squid64
tcp 0 0 140. 161.29795 128.199.131.10:22 ESTABLISHED 1040/squid64
tcp 0 1 140. 161.49221 165.77.189.195:22 SWN_SENT 9595/squid64
tcp 0 144 140. 161.43674 196.29.129.5:22 ESTABLISHED 8885/squid64
tcp 0 1 140. 161.50128 6.107.104.39:22 SWN_SENT 9392/squid64
tcp 0 1 140. 161.81542 215.11.166.41:22 SWN_SENT
tcp 0 1 140. 161.50245 35.2.146.71:22 SWN_SENT 9392/squid64
tcp 0 1 140. 161.41233 16.164.122.50:22 SWN_SENT 8781/squid64
tcp 0 68 140. 161.59055 54.82.243.2:22 ESTABLISHED 9392/squid64
tcp 0 100 140. 161.45246 203.196.133.100:22 ESTABLISHED 9392/squid64
tcp 0 21 140. 161.54282 176.73.166.45:22 ESTABLISHED 9188/squid64
tcp 0 21 140. 161.50115 83.46.80.25:22 ESTABLISHED 9798/squid64
tcp 0 0 140. 161.36470 65.210.45.81:22 ESTABLISHED 1000/squid64
tcp 0 1 140. 161.40557 161.139.122.9:22 ESTABLISHED 9595/squid64
tcp 0 1 140. 161.42319 197.6.244.139:22 SWN_SENT 9392/squid64
tcp 0 52 140. 161.56821 118.173.44.59:22 ESTABLISHED 9798/squid64
tcp 0 1 140. 161.41336 190.6.244.5:22 SWN_SENT 9595/squid64
tcp 0 0 140. 161.41764 91.18.234.195:22 ESTABLISHED 9392/squid64
tcp 0 1 140. 161.40086 60.34.79.106:22 SWN_SENT
tcp 0 144 140. 161.47471 81.21.104.17:22 ESTABLISHED 9798/squid64
tcp 0 0 140. 161.34626 65.210.45.81:22 ESTABLISHED 9392/squid64
tcp 0 1 140. 161.58342 87.254.89.170:22 SWN_SENT 9188/squid64
tcp 0 1 140. 161.84570 55.4.152.179:22 SWN_SENT 9885/squid64
tcp 0 1 140. 161.33601 130.47.201.251:22 SWN_SENT 9188/squid64
tcp 0 21 140. 161.57541 201.218.62.65:22 ESTABLISHED 9595/squid64
tcp 0 0 140. 161.42505 83.60.54.157:22 ESTABLISHED 1040/squid64
tcp 0 0 140. 161.58047 173.165.146.119:22 ESTABLISHED 9798/squid64
```

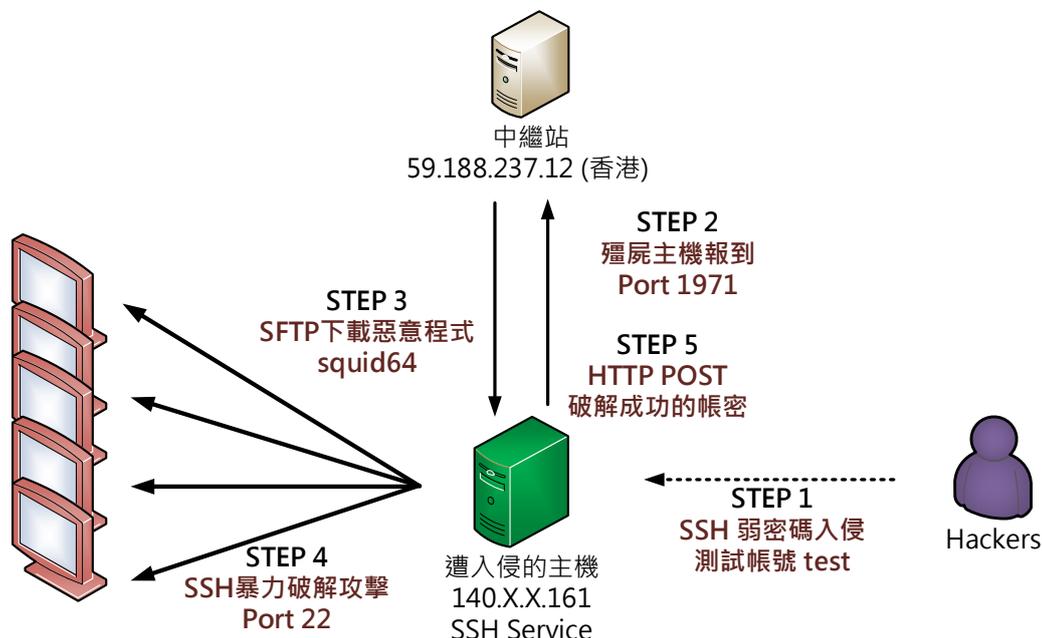
圖 6.

...



資安事件個案分析-Y 大學大量對外進行 SSH 攻擊的主機事件分析報告-2

※ 網路架構圖：



※ 運作流程

- 一. 駭客透過 SSH 弱密碼入侵學校主機，並使用測試帳號 test 登入。
- 二. 被入侵主機回報主機資料給中繼站。
- 三. 駭客從中繼站下載惡意程式 squid64 並執行後刪除檔案。
- 四. 主機產生十個 squid64 的 PID 持續對外部大量主機進行 SSH 暴力破解。
- 五. 破解成功的主機帳號密碼透過 HTTP POST 方式回傳給中繼站。

※ 建議與總結：

- 一. 此案例主機因為測試帳號 test 維護完後並未完全移除，而只移除了帳號的家目錄。
- 二. 該主機預設有開啟 SSH server 服務讓管理者連入，然而並未限制連入來源端 IP，導致駭客利用帳號 test 以及弱密碼入侵成功。
- 三. 駭客 SSH 入侵後雖不能存取 root 權限，但能透過 SFTP 向香港中繼站下載惡意程式 squid64，並且大量去對外部主機進行 SSH 破解攻擊。
- 四. SSH 外部攻擊時將破解成功的主機帳號密碼透過 HTTP POST 方式傳輸給上層香港中繼站。
- 五. 對外 SSH 破解攻擊時占用大量網路頻寬，導致單位對外網路壅塞影響其他人網路使用。
- 六. 惡意程式排除方式為，因惡意程式 squid64 主體駭客執行完就已經移除，故只須將正在執行的惡意程式 squid64 的 PID 程序依序 kill 刪除。
- 七. 漏洞修補方式則是透過將帳號 test 徹底從 /etc/passwd 中移除。
- 八. 設定 SSH 來源端登入限制，限制特定網段或 IP 能夠存取，避免駭客再次入侵，或者加強帳號的密碼強度防止輕易被破解。

*[詳細完整個案分析報告，請參閱 TACERT 網站！](#)



資安事件個案分析-P 大學遭植入惡意後門程式的主機事件分析報告-1

※ 前言：

- 一. 該校主機系統管理人員發現該主機疑似有可疑程式在背景執行。
- 二. 該系統使用 Linux 系統，並作為重要對外服務用的系統主機。由於該主機為重要設備，管理者已先行將惡意程式移除。
- 三. 管理者並將惡意程式樣本請本單位協助分析，以了解惡意程式的可能行為。
- 四. 本單位所使用的惡意程式測試環境為 Win7 及 Linux Centos。

※ 事件檢測

- 一. 取得的惡意程式樣本中，主要有 test.py 和 test.exe 兩支程式，主要功能為建立環境的腳本程式。
- 二. test.exe 為一個自解壓縮執行檔，需在 windows 系統下執行，內容分別為「_wpcap_. bat、npf. sys、Packet. dll、SCServ. exe、wpcap. dll」五個檔案(如圖 7 所示)。
- 三. 從「_wpcap_. bat」中可知該檔案為建立環境腳本，將必要的工具檔案複製到系統中後，主要以惡意程式 SCServ. exe 為惡意連線程式。
- 四. 如圖 8 所示，透過 procexp 工具查看背景程式執行狀況，惡意程式 SCServ. exe 的檔案描述和發布廠商是空白的，並且在 virustotal 上有被偵測出 3/57 的比例是異常。
- 五. 如圖 9 所示，透過 autoruns 工具查看程式開機時狀態，SCServ. exe 被寫入系統 service 機碼中啟用。
- 六. 透過 virustotal 檢測 SCServ. exe，檢測出的比例 3/57 相當低(圖 10)，只要三家防毒軟體有偵測出為木馬後門程式，這些防毒軟體在台灣幾乎很少人使用。
- 七. 檢測 test.exe 執行後，會自動先執行批次檔「_wpcap_. bat」，隨後執行惡意程式 SCServ. exe，觀察側錄的網路封包行為得知，惡意程式不會直接向特定 IP 報到，而是透過網域名稱跳板連線。
- 八. 惡意程式會先 DNS 查詢網址「live. cakverd. com」(如圖 11 所示)，然而該網域早已失效，故此連線並不成功，觀察不到後續行為。
- 九. 該惡意程式 SCServ. exe 會存在於資料夾 C:\Program Files\ 中，並且寫入開機服務區自動啟用，如圖 12 所示。
- 十. 因在 windows 的環境中無法明確得知惡意程式的網路行為，故同時測試 test.py 在 Linux 環境中的運作行為。



圖 7. test.exe 解壓縮後

Process	CPU	Private	Working	Description	Company N...	VerasT...	Verifie...
SearchIndex	23.53	2072	2	Microsoft Wi...	Microsoft C...	057	(Verifie...
svchost.exe	5.676 K	9,328 K	2	Windows Me...	Microsoft C...	057	(Verifie...
svchost.exe	2,392 K	6,120 K	2	Windows Ser...	Microsoft C...	057	(Verifie...
svchost.exe	63.97	18,888	820	Windows Ser...	Microsoft C...	057	(Verifie...
SCServ.exe	1,012 K	2,740 K	1				
lsass.exe	13.31	18.31				287	(空)
lsass.exe	3,468 K	8,880 K	520	Local Secur...	Microsoft C...	Unknown	(Verifie...
lsim.exe	0	2,164 K	3,496 K	532			

圖 8. 利用 procexp 工具檢測

Autrun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Services			
SCServ			c:\program files\scserv.exe

圖 9. 利用 autoruns 工具檢測

SHA256	21846842e7148b9d0061067611dbcc5725ef8eada69310c759e5b128c969e462
檔案名稱	SCServ.exe
偵測率	3 / 57
分析日期	2015-05-25 03:57:04 UTC (3 小時, 24 分鐘前)
防病毒	結果
AhnLab-V3	Trojan.Win32.Sarrot
Tencent	Trojan.Win32.YY.Gen.0
TheHacker	Backdoor/Sarrot.H

圖 10. virustotal 檢測結果

Time	Source	Destination	Protocol	Length	Info
1 0.0000140	192.168.1.1	8.8.8.8	DNS	76	Standard query 0x1c4cf live.cakverd.com
2 0.0000140	192.168.1.1	8.8.8.8	DNS	149	Standard query response 0x1c4cf no such name

圖 11.

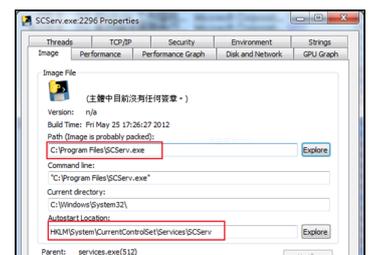
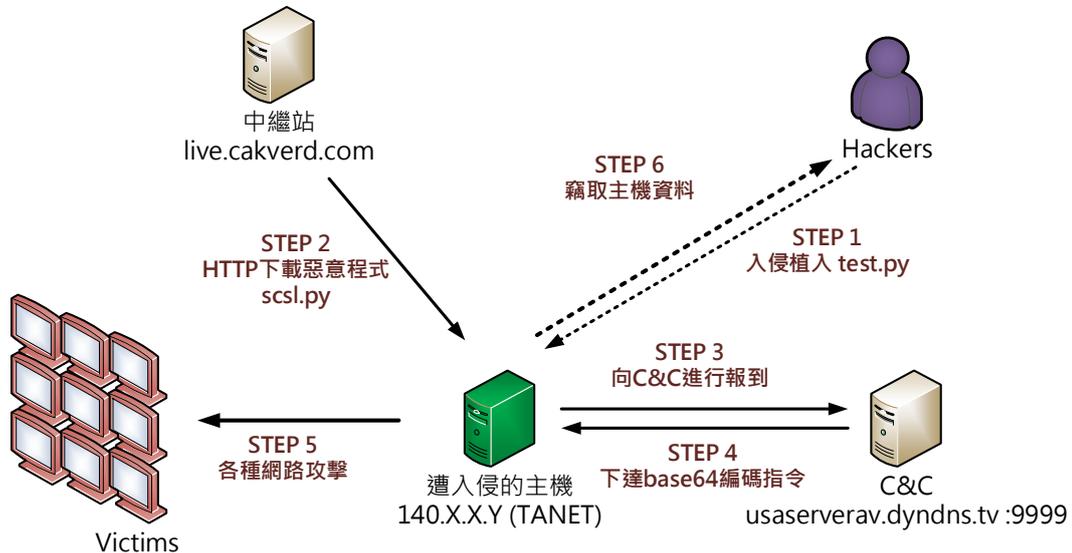


圖 12.



資安事件個案分析-P 大學遭植入惡意後門程式的主機事件分析報告-2

※ 網路行為架構圖：



- 一. 駭客透過某種方式入侵並植入 test.py 的程式。
- 二. 主機執行 test.py 後會向 live.cakverd.com 下載 scsl.py 惡意程式。
- 三. Scsl.py 執行後會向上層 C&C 報到等待指令。
- 四. C&C 會下達控制指令進行網路攻擊等動作。
- 五. 主機開始向外部進行網路攻擊。
- 六. 駭客也能隨時竊取主機內的檔案資料。

※ 建議與總結：

- 一. 由於此案例並無實際接觸到原始受害主機，無法得知該病毒確切入侵方式，推測可能是透過 SSH 或 TELNET 遠端登入植入。
- 二. 排除方式先將該背景程式用 kill 指令關閉，並將 /bin/scsl.py 檔案移除，以及開機啟動區中 /etc/rc.local 內的 scsl.py 啟用移除。
- 三. 透過病毒樣本測試分析，得知駭客可能夠取得 root 權限進行遠端控制，並且透過感染主機進行對外攻擊或竊取資料。
- 四. 惡意程式中所連線的上層 C&C 伺服器並非直接透過 IP 連線，而是透過 DNS 網域名稱解析連線，此好處是一旦網址失效舊追查不到確切 IP 位址。
- 五. 該惡意程式原始碼於網路上公布的時間為 2014 年上半年，推測受害主機遭受感染可能有半年以上。
- 六. 由於該主機並無直接對外的 Web 服務，建議若有 SSH 或 TELNET 服務務必限制登入來源端 IP。
- 七. 加強系統的帳號及密碼強度，避免容易被猜測入侵。
- 八. 時常檢查系統的登入 LOG 紀錄及背景開啟程式及網路通訊埠，以減少被感染的可能性。

[*詳細完整個案分析報告，請參閱TACERT網站！](#)



資安新知-SSDP 及 UPnP 漏洞攻擊

簡單服務發現協定 (Simple Service Discovery Protocol ; SSDP) 是一種應用層協定，是構成通用隨插即用 (UPnP) 技術的核心協定之一。使用範圍廣泛加上預設為啟動，容易成為攻擊目標，包括路由器、媒體伺服器、網絡攝影機、智能電視和列印機，透過網絡彼此連接，建立溝通和協調活動。若有任何未被保護或配置錯誤的，這些以家用為主和連接互聯網的裝置可用作為反射器，進而被利用成為 DDoS 攻擊的工具。路由器尤其可能成為首要攻擊目標，因為攻擊者可以改變 DNS 設定，將設備導向被攻擊者控制的伺服器，然後透過該路由器散布垃圾郵件、或是進行點擊劫持詐騙(clickjacking scam)以獲取利益，甚至監控該設備的網路流量等。

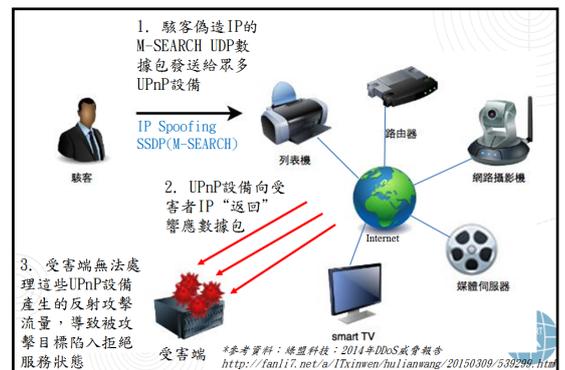


圖 13.SSDP 反射式 DDoS 攻擊分析圖

- 預防方法：① 設置防火牆策略 (考慮配置防火牆規則，並停止 UDP 1,900 連接埠的存取)
 ② 停用路由器的 UPnP 功能。③ 安裝更新及修補 UPnP 漏洞。④ 最佳的安全做法，使用者不應開啟任何不需要的功能。

參考資料：[HKCERT-通用隨插即用\(UPnP\)功能服務顯露，潛在危機四伏](#)

TACERT 組織介紹

臺灣學術網路危機處理中心(TANet Computer Emergency Response Team, 簡稱 TACERT)於 2010 年 6 月正式成立，由教育部委由國立中山大學進行營運。主要的任務為協助處理 TANet 各連線單位的電腦網路資通安全危安事件。除了扮演教育體系的資訊安全應變窗口，並盡力維護台灣學術網路的使用安全。

TACERT 主要營運項目包含：(1)資安事件的通報應變(2)資安事件的技術支援與諮詢服務(3)資安預警情資(4)資安防護教育訓練



圖 14.TACERT 網站

臺灣學術網路危機處理中心(TACERT)

電話：(07)525-0211 傳真：(07)525-1535

網路電話代表號：98400000

電子郵件：service@cert.tanet.edu.tw

地址：高雄市鼓山區蓮海路 70 號(國立中山大學)

