個案分析-

phpMyAdmin setup.php

分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/05

前言

PhpMyadmin[1]是一個以 PHP 語言為基礎，讓使用者可以透過 Web 介面管理後端 Mqsql 資料庫的套件，它提供了許多管理功能，如資料庫匯入、匯出、刪除、修改等，讓使用者在管理後端資料庫上省下許多時間。

PhpMyadmin 常與 Apache、PHP、Mysql 這三個套件一起安裝，由於使用者需求，多年前網路上流行著一個架站整合套件 AppServ[2]，AppServ 整合了 PhpMyadmin、Apache、PHP、Mysql，並且在安裝時自動幫使用者將 Apache、PHP、Mysql 與 PhpMyAdmin 四個套件設定好，使用者僅需要輸入資料庫的帳號密碼便可，由於這樣的便利性，即使 AppServ 已經五年沒有更新（最後一次更新時間為 2008-06-10），仍有許多大專院校學生在架站時使用這個整合套件。

事件說明

2013 年 3 月開始，D 大學資工系所使用的網段 IP 一直收到四種不同的 EWA 事件單：

- udp_flood
- udp_scan
- udp_src_session
- ip_dst_session

約有三十個 IP 一直被重複開單，由於網段管理員查不出原因，而這些事件單幾乎每天都有，一次多達五十張以上，因而引起該校資安聯絡人注意。這些被開單的 IP 位於下列這些網段：

- xxx.208.2.0/24
- xxx.208.3.0/24
- xxx.208.6.0/25

被開單的主機皆裝有 AppServ 2.5.10，安裝路徑使用預設，AppServ 預設路徑會安裝在 C 槽底下，由於都使用預設安裝路徑，所以這些被開單的主機不約而同都有這個頁面 http://xxx.208.x.x/phpmyadmin/scripts/setup.php（如圖 1），由 Apache 的 Log 可以看到，14.139.56.12 這個 IP 利用 setup.php 頁面成功 POST 某些參數，（圖 2 可以看到伺服器回應碼 200）。

而從主機的流量中則可以發現，14.139.56.12 利用這個方法，對 xxx.208.2.217 注入了某些 code，使得主機會自動下載一個惡意的 phpBot，並且使 httpd.exe 執行之。由於是透過 httpd.exe 執行 phpBot，當攻擊發生時，由主機的網路狀態看起來像是 httpd.exe 這個程式去攻擊別人。

圖 1 預設安裝路徑下的 setup.php 頁面

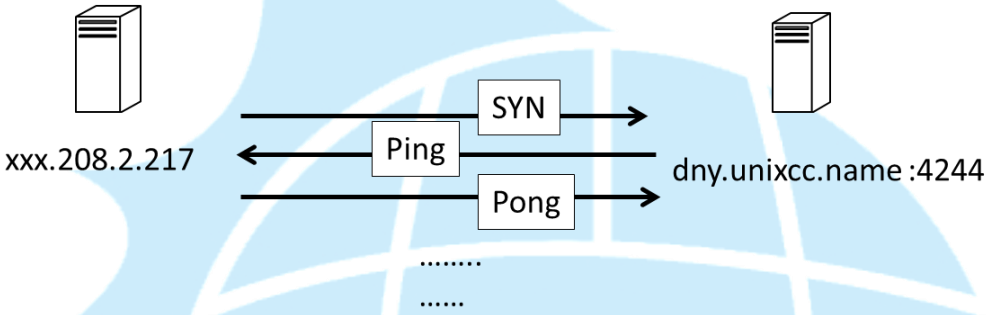
```
14.139.56.12 - - [15/Mar/2013:00:03:57 +0800] "POST /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 430999
14.139.56.12 - - [15/Mar/2013:00:04:01 +0800] "POST /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 430999
14.139.56.12 - - [15/Mar/2013:00:04:01 +0800] "POST /phpmyadmin/scripts/setup.php HTTP/1.1" 200 450996
14.139.56.12 - - [15/Mar/2013:00:04:05 +0800] "POST /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 430999
14.139.56.12 - - [15/Mar/2013:00:04:04 +0800] "POST /phpmyadmin/scripts/setup.php HTTP/1.1" 200 430999
```

圖 2 xxx.208.2.217 的 Web Log 中，可以看到駭客經由 setup.php 頁面成功 POST 資料

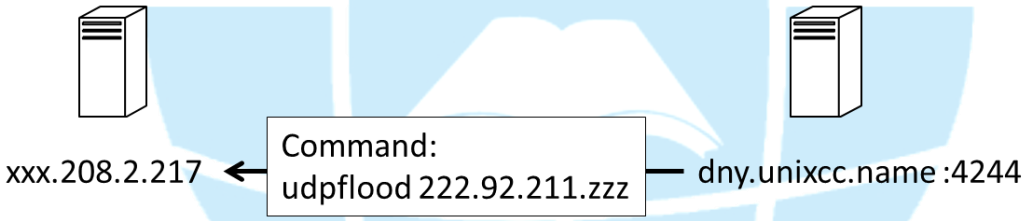
事件發生流程

Step 1:駭客利用setup.php頁面的漏洞，迫使主機下載phpBot 並執行之

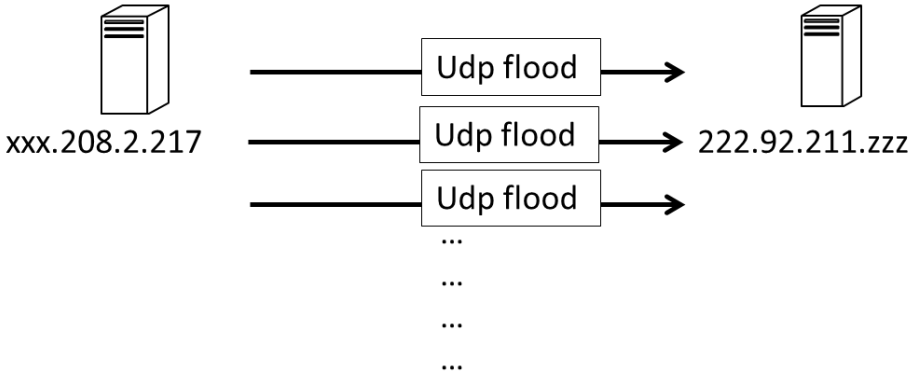
Step 2:「phpBot 」執行後會連往IRC主機，等候命令



Step 3:IRC主機會在特定時間傳送攻擊命令給xxx.208.2.217



Step 4:當xxx.208.2.217收到命令，便會對特定目標發動UDP FLOOD而引發大量的EWA事件單產生



建議措施

1. 刪除 C:\AppServ\www\phpMyAdmin\scripts\setup.php （這是預設路徑，有的主機 setup.php 可能不在此路徑下）
2. 重新啟動主機（務必重新啟動主機以清空記憶體裡的攻擊程式）
3. 備份資料，重新安裝最新版的 Apache、PHP、Mysql、PhpMyAdmin

由於學校資工系的學生慣用 AppServ 架站，所以九成以上發出大量 UDP 封包的主機都來自該校的資工系網域，有些主機甚至為重要的網站及服務主機，難以在短時內備份，並重新安裝 Apache、PHP、Mysql、PhpMyAdmin。

由於這些主機發動 UDP Flood 的惡意程式是透過 setup.php 的漏洞注入主機，關機之後惡意程式就會從記憶體裡面消失，所以只要電腦重開機，便看不出任何可疑的地方，等到下次駭客需要進行攻擊，才會再利用 setup.php 頁面，注入 phpBot 到主機裡面進行攻擊。

因此，管理員可以利用 1)刪除 setup.php 2)重新開機，兩個步驟，讓駭客不能注入惡意程式到主機裡面，並且重開機將記憶體裡面的 phpBot 揮發掉。由於不曉得駭客是否利用 setup.php 頁面在主機裡面設置了其他的惡意程式，備份主機資料，重灌系統，並且安裝最新版的 Apache、PHP、Mysql、PhpMyAdmin 才是最好的解決之道。

參考

[1] http://www.phpmyadmin.net/home_page/index.php

[2] http://www.appservnetwork.com/