個案分析-

# 校園網站伺服器淪為駭客練兵場事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

107 年 8 月

# I. 事件簡介

1. 本次事件是某學校的英語自學網站伺服器被駭客入侵後，對外進行 Web.Server.Password.Files.Access 攻擊的事件。從資安通報事件單內容，可以得知該事件的觸發時間點在 2018 年 6 月 16 日 10:50:39。

事件單編號:AISAC-1[redacted]0

| | | | |
|---|---|---|---|
| 原發布編號 | ASOC-INT-2018[redacted]9 | 原發布時間 | 2018-06-19[redacted] |
| 事件類型 | 對外攻擊 | 原發現時間 | 2018-06-16 10:50:39 |
| 事件主旨 | 通報:[redacted]140.[redacted].92 Web.Server.Password.Files.Access | | |
| 事件描述 | ASOC發現貴單位([redacted])所屬 140.[redacted].92 疑似對外進行 Web.Server.Password.Files.Access 攻擊 | | |
| 手法研判 | 貴單位疑似對外進行非法的入侵攻擊，利用被攻擊者端未對/etc/passwd檔案進行完善的安全性設定，使用HTTP、FTP、SMB等服務來非法存取/etc/passwd檔案，並利用暴力攻擊法破解使用者密碼，進而取得使用者的帳密來進行非法存取。 受影響範圍：所有未防護的Web伺服器 | | |
| 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。 2.利用工具程式於來源主機觀察，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。 5.攻擊名稱相關參考資料網站： http://www.fortinet.com/ids/VID43336 http://www.iss.net/security_center/reference/vuln/temp/HTTP_Unix_Passwords.htm | | |

2. 受害主機為英語自學網站，平時主要提供校內學生自學英語使用，有提供學生登入系統與上傳作業的功能，可能為駭客入侵的管道。


3. 為了解受害主機被駭客入侵情形與駭客入侵後之行為，本中心進行實機檢測與封包側錄。

## II. 事件檢測

1. 首先，檢視受害主機內「伺服器管理員」的內容，得知下面資訊:

   (1) 受害主機使用 Windows Server 2016 的作業系統。

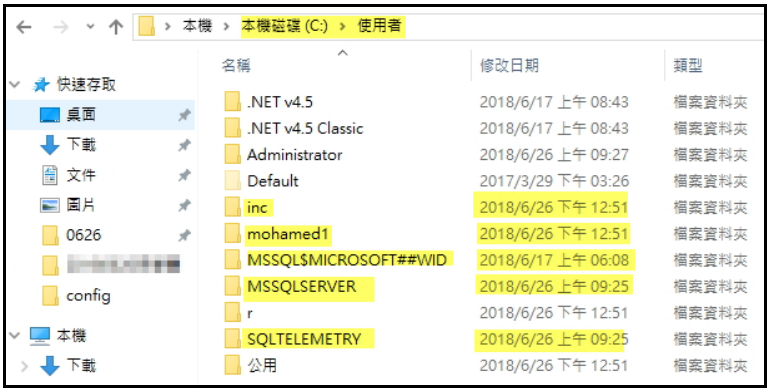
   (2) 有使用 Windows update 下載更新。

   (3) 有啟用遠端桌面服務，但卻未限制連入的來源端 IP 或網段。

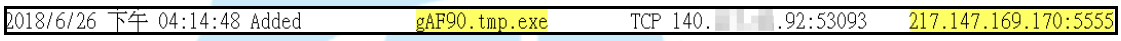
   (4) 未使用微軟內建 Windows Defender 防毒軟體，查看整台主機也未發現有安裝防毒軟體。


2. 查看使用者帳戶資訊，發現在受害主機的本機帳戶內被新增一個不知來源的使用者 mohamed1，而且具有系統管理員權限。在檢測期間，也發現駭客又新增另一個具有系統管理員權限的使用者 b3r。

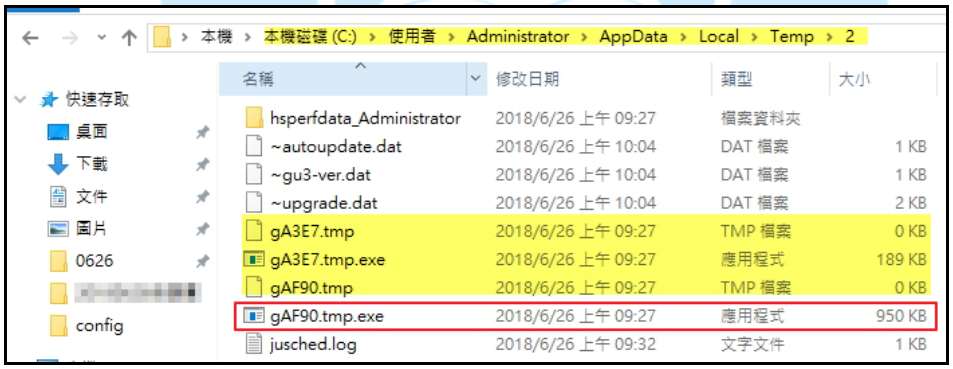

3. 查看 C:\使用者資料夾，發現被建立許多不明來源的資料夾，推測為駭客入侵後所建立。

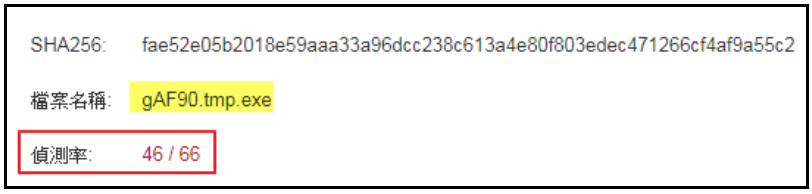



4. 檢視受害主機對外連線狀況，發現有一個不明來源的程式 gAF90.tmp.exe 會對外連線烏克蘭 IP:217.147.169.170:5555，port 5555 為挖礦程式常用的 port，推測該程式可能為一個挖礦程式。




5. 查看程式 gAF90.tmp.exe 所在位置，發現位於 C:\Users\ADMINI~1\AppData\Local\Temp\2 內，在該資料夾中也發現另一個程式 gA3E7.tmp.exe。經 Virustotal 檢測，程式 gAF90.tmp.exe 與 gA3E7.tmp.exe 的惡意比例分別為 46/66 與 54/67，其中 gAF90.tmp.exe 被多家防毒軟體公司視為挖礦程式。

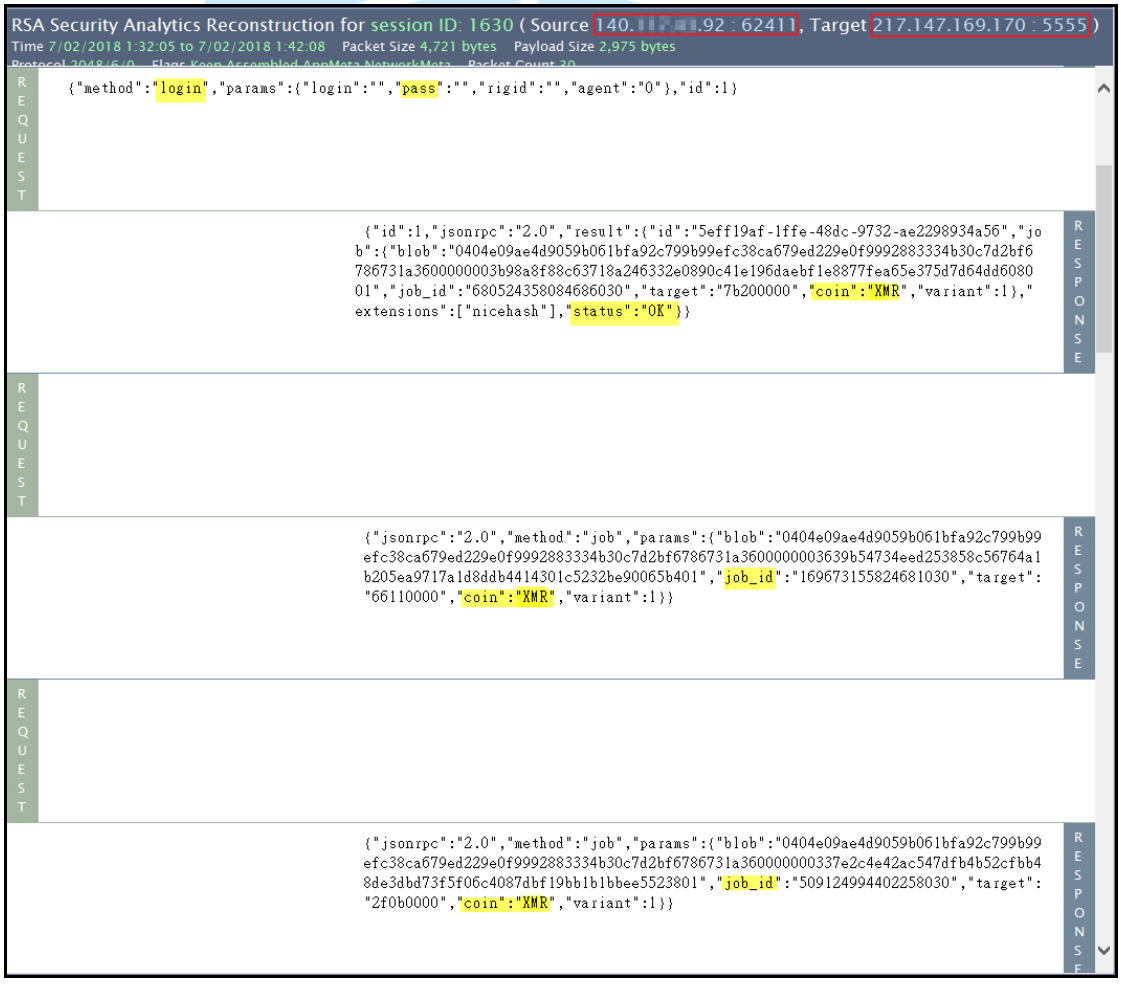



| | |
|---|---|
| ESET-NOD32 | a variant of Win64/CoinMiner.KJ |
| F-Secure | Trojan.GenericKD.30944790 |
| Fortinet | W64/CoinMiner.KJ!tr |
| GData | Trojan.GenericKD.30944790 |
| Ikarus | PUA.CoinMiner |

| | |
|---|---|
| SHA256: | 280c708ccb56b6ee1aea68dfb618774471e17b2e478a14bf199cd717fed20a67 |
| 檔案名稱: | gA3E7.tmp.exe |
| 偵測率: | 54 / 67 |

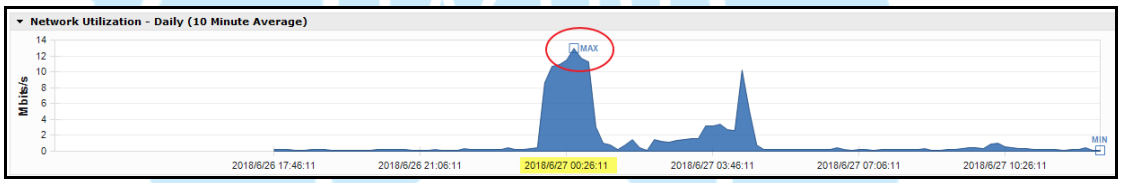
6. 從封包內容可以看到受害主機連線 IP:217.147.169.170，進行登入礦池，並開始挖礦作業的動作。




7. 查看受害主機的網站存取紀錄，發現有來自突尼西亞 IP:197.2.253.30 的頻繁存取紀錄，而且都存取成功。從其存取的途徑可以知道該 IP 透過網站 upload 資料夾執行 cmd、bypass、upload、edit、newfile、delete…的指令，

並且讀取一些 php 檔，例如:bl.php、rdp.php，可見駭客透過網站的 upload 資料夾駭入受害主機來執行 PHP WebShell 指令。


8. 使用網路分析儀側錄封包，發現在 2018 年 6 月 27 日凌晨有大量封包流量進出，而且有許多來自突尼西亞(Tunisia)的連線，其中有 3 個 IP 有可疑的封包流量，分別是 IP:197.28.167.13、197.2.253.30 與 196.229.63.112。




| Node | Country | Total Bytes % | Total Bytes | Packets Sent | Packets Received |
|---|---|---|---|---|---|
| 197.29.254.246 | Tunisia | 0.000% | 7,211 | 51 | 54 |
| 197.29.17.141 | Tunisia | 0.000% | 350 | 5 | 0 |
| 197.29.13.10 | Tunisia | 0.000% | 1,470 | 21 | 0 |
| 197.28.184.169 | Tunisia | 0.000% | 70 | 1 | 0 |
| 197.28.167.13 | Tunisia | 0.177% | 19,257,047 | 25,536 | 33,592 |
| 197.26.110.177 | Tunisia | 0.000% | 70 | 1 | 0 |
| 197.25.177.144 | Tunisia | 0.000% | 1,214 | 8 | 6 |
| 197.18.150.209 | Tunisia | 0.000% | 11,109 | 43 | 94 |
| 197.15.63.29 | Tunisia | 0.000% | 821 | 5 | 4 |
| 197.15.34.131 | Tunisia | 0.000% | 975 | 6 | 5 |
| 197.14.253.230 | Tunisia | 0.000% | 70 | 1 | 0 |
| 197.14.145.33 | Tunisia | 0.000% | 70 | 1 | 0 |
| 197.14.131.18 | Tunisia | 0.000% | 907 | 6 | 4 |
| 197.9.205.154 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.9.161.34 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.9.112.158 | Tunisia | 0.000% | 140 | 2 | 0 |
| 197.9.81.166 | Tunisia | 0.000% | 340 | 1 | 4 |
| 197.9.69.106 | Tunisia | 0.000% | 70 | 1 | 0 |
| 197.9.4.119 | Tunisia | 0.000% | 1,595 | 6 | 7 |
| 197.8.107.85 | Tunisia | 0.000% | 410 | 2 | 4 |
| 197.8.28.184 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.7.147.26 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.7.143.168 | Tunisia | 0.000% | 594 | 5 | 4 |
| 197.7.136.175 | Tunisia | 0.000% | 268 | 2 | 2 |
| 197.6.253.128 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.6.221.116 | Tunisia | 0.000% | 340 | 4 | 1 |
| 197.6.218.237 | Tunisia | 0.000% | 70 | 1 | 0 |
| 197.6.153.98 | Tunisia | 0.000% | 1,420 | 8 | 7 |
| 197.6.63.31 | Tunisia | 0.000% | 70 | 0 | 1 |

| Node | Country | Total Bytes % | Total Bytes | Packets Sent | Packets Received |
|---|---|---|---|---|---|
| 197.5.59.204 | Tunisia | 0.000% | 1,167 | 8 | 5 |
| 197.4.73.74 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.4.40.131 | Tunisia | 0.000% | 340 | 1 | 4 |
| 197.4.29.23 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.4.18.75 | Tunisia | 0.000% | 480 | 3 | 4 |
| 197.4.1.97 | Tunisia | 0.000% | 70 | 0 | 1 |
| 197.3.230.87 | Tunisia | 0.000% | 945 | 6 | 4 |
| 197.3.211.183 | Tunisia | 0.000% | 480 | 3 | 4 |
| 197.3.211.92 | Tunisia | 0.000% | 2,695 | 16 | 22 |
| 197.2.253.30 | Tunisia | 0.524% | 57,058,302 | 83,855 | 102,927 |
| 197.2.201.227 | Tunisia | 0.000% | 9,369 | 68 | 64 |
| 197.2.162.68 | Tunisia | 0.000% | 1,157 | 8 | 7 |
| 197.2.6.61 | Tunisia | 0.000% | 480 | 3 | 4 |
| 197.1.174.137 | Tunisia | 0.000% | 1,231 | 8 | 7 |
| 197.1.60.129 | Tunisia | 0.000% | 338 | 3 | 2 |
| 197.1.12.109 | Tunisia | 0.000% | 340 | 2 | 3 |
| 197.1.7.237 | Tunisia | 0.001% | 100,637 | 731 | 727 |
| 197.1.6.37 | Tunisia | 0.000% | 340 | 1 | 4 |
| 197.1.3.235 | Tunisia | 0.000% | 49,409 | 354 | 355 |
| 197.0.121.220 | Tunisia | 0.000% | 70 | 1 | 0 |
| 197.0.95.6 | Tunisia | 0.000% | 979 | 7 | 5 |
| 197.0.94.90 | Tunisia | 0.000% | 1,111 | 8 | 5 |
| 197.0.16.87 | Tunisia | 0.000% | 70 | 1 | 0 |

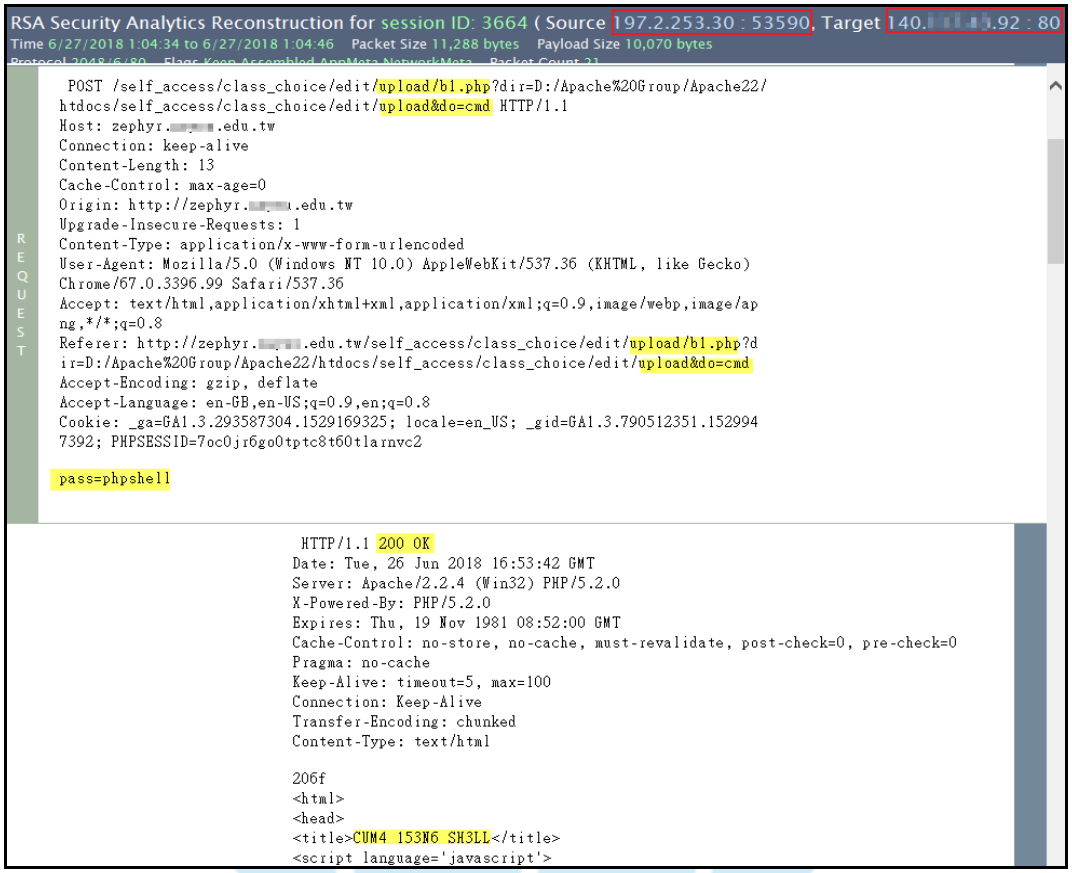
| Node | Country | Total Bytes % | Total Bytes | Packets Sent | Packets Received |
|---|---|---|---|---|---|
| 196.234.201.70 | Tunisia | 0.000% | 70 | 1 | 0 |
| 196.234.174.34 | Tunisia | 0.000% | 1,129 | 10 | 5 |
| 196.234.171.121 | Tunisia | 0.000% | 460 | 4 | 3 |
| 196.229.239.3 | Tunisia | 0.000% | 813 | 5 | 4 |
| 196.229.192.192 | Tunisia | 0.000% | 70 | 1 | 0 |
| 196.229.63.112 | Tunisia | 0.732% | 79,743,204 | 104,347 | 128,580 |
| 196.229.17.158 | Tunisia | 0.000% | 873 | 7 | 4 |
| 196.224.136.177 | Tunisia | 0.000% | 1,674 | 6 | 16 |

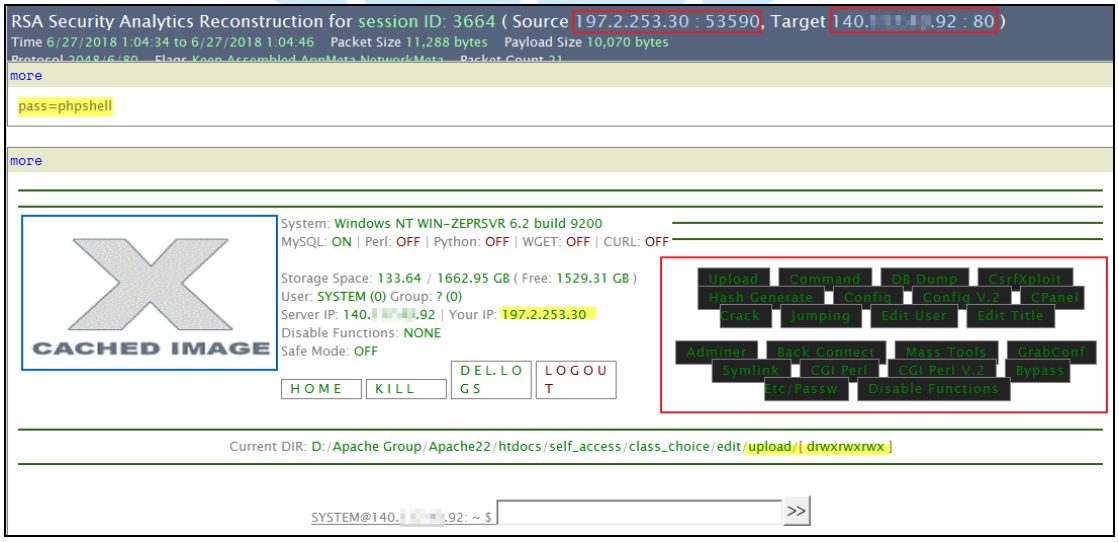
9. 檢視所側錄的封包可以看到在 2018 年 6 月 27 日凌晨一點起有多筆來自 IP:197.2.253.30 的連線，連到受害主機的 80 port，推斷駭客透過網頁方式侵入受害主機。

| Time | Service | Size | Events | Displaying 1 - 150 of 160 |
|---|---|---|---|---|
| 2018-Jun-27 01:01:46 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53283 -> 80 (http) |
| 2018-Jun-27 01:01:46 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53281 -> 80 (http) |
| 2018-Jun-27 01:01:46 | IP / TCP / HTTP | 2.72 KB | 197.2.253.30 -> 140. .92 | 53282 -> 80 (http) |
| 2018-Jun-27 01:04:24 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53568 -> 80 (http) |
| 2018-Jun-27 01:04:21 | IP / TCP / HTTP | 2.70 KB | 197.2.253.30 -> 140. .92 | 53571 -> 80 (http) |
| 2018-Jun-27 01:04:34 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53593 -> 80 (http) |
| 2018-Jun-27 01:04:34 | IP / TCP / HTTP | 11.02 KB | 197.2.253.30 -> 140. .92 | 53590 -> 80 (http) |
| 2018-Jun-27 01:04:51 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53622 -> 80 (http) |
| 2018-Jun-27 01:04:51 | IP / TCP / HTTP | 21.33 KB | 197.2.253.30 -> 140. .92 | 53619 -> 80 (http) |
| 2018-Jun-27 01:06:39 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53849 -> 80 (http) |
| 2018-Jun-27 01:06:39 | IP / TCP / HTTP | 38.11 KB | 197.2.253.30 -> 140. .92 | 53848 -> 80 (http) |
| 2018-Jun-27 01:07:14 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53908 -> 80 (http) |
| 2018-Jun-27 01:07:13 | IP / TCP / HTTP | 9.68 KB | 197.2.253.30 -> 140. .92 | 53907 -> 80 (http) |
| 2018-Jun-27 01:07:22 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53923 -> 80 (http) |
| 2018-Jun-27 01:07:32 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53937 -> 80 (http) |
| 2018-Jun-27 01:07:32 | IP / TCP / HTTP | 17.94 KB | 197.2.253.30 -> 140. .92 | 53940 -> 80 (http) |
| 2018-Jun-27 01:08:01 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 53991 -> 80 (http) |
| 2018-Jun-27 01:08:01 | IP / TCP / HTTP | 21.86 KB | 197.2.253.30 -> 140. .92 | 53988 -> 80 (http) |
| 2018-Jun-27 01:08:23 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 54024 -> 80 (http) |
| 2018-Jun-27 01:08:35 | IP / TCP / HTTP | 2.37 KB | 197.2.253.30 -> 140. .92 | 54043 -> 80 (http) |
| 2018-Jun-27 01:09:15 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 54109 -> 80 (http) |
| 2018-Jun-27 01:09:15 | IP / TCP / HTTP | 1.33 KB | 197.2.253.30 -> 140. .92 | 54110 -> 80 (http) |
| 2018-Jun-27 01:09:30 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 54137 -> 80 (http) |
| 2018-Jun-27 01:09:46 | IP / TCP / OTHER | 432 B | 197.2.253.30 -> 140. .92 | 54165 -> 80 (http) |
| 2018-Jun-27 01:10:35 | IP / TCP / HTTP | 40.16 KB | 197.2.253.30 -> 140. .92 | 54246 -> 80 (http) |

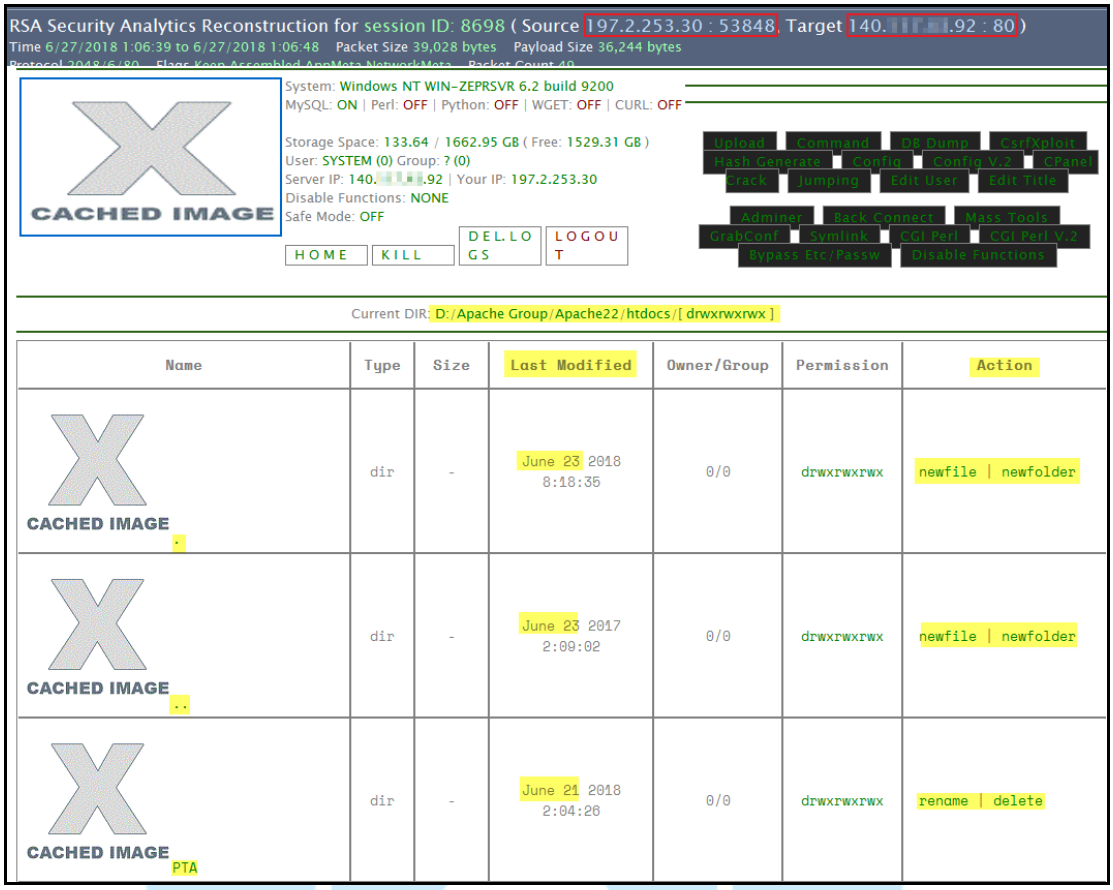
10. 分析來自突尼西亞 IP:197.2.253.30 的封包內容，得知該 IP 在連線後，讀取 upload 資料夾的一些 php 檔，並執行一些指令，分析如下:

(1)透過 b1.php 執行 cmd 指令 pass=phpshell 成功，而且從 b1.php 頁面可以知道此 php 檔含有許多執行指令的工具，像 upload、command、DB dump…，駭客可以透過此方式完全掌握受害主機。



(2)從封包內容可以看到來自突尼西亞的駭客對受害主機的網站各資料所進行的提權修改紀錄，將這些資料夾提權到管理者的最大權限。




| Name | Type | Size | Last Modified | Owner/Group | Permission | Action |
|---|---|---|---|---|---|---|
| CACHED IMAGE . | dir | - | June 23 2018 8:18:35 | 0/0 | drwxrwxrwx | newfile \| newfolder |
| CACHED IMAGE .. | dir | - | June 23 2017 2:09:02 | 0/0 | drwxrwxrwx | newfile \| newfolder |
| CACHED IMAGE PTA | dir | - | June 21 2018 2:04:26 | 0/0 | drwxrwxrwx | rename \| delete |
| CACHED IMAGE self_access | dir | - | June 22 2018 7:08:12 | 0/0 | drwxrwxrwx | rename \| delete |
| CACHED IMAGE splendid | dir | - | June 21 2018 2:04:26 | 0/0 | drwxrwxrwx | rename \| delete |
| CACHED IMAGE tmp | dir | - | June 25 2018 11:55:51 | 0/0 | drwxrwxrwx | rename \| delete |

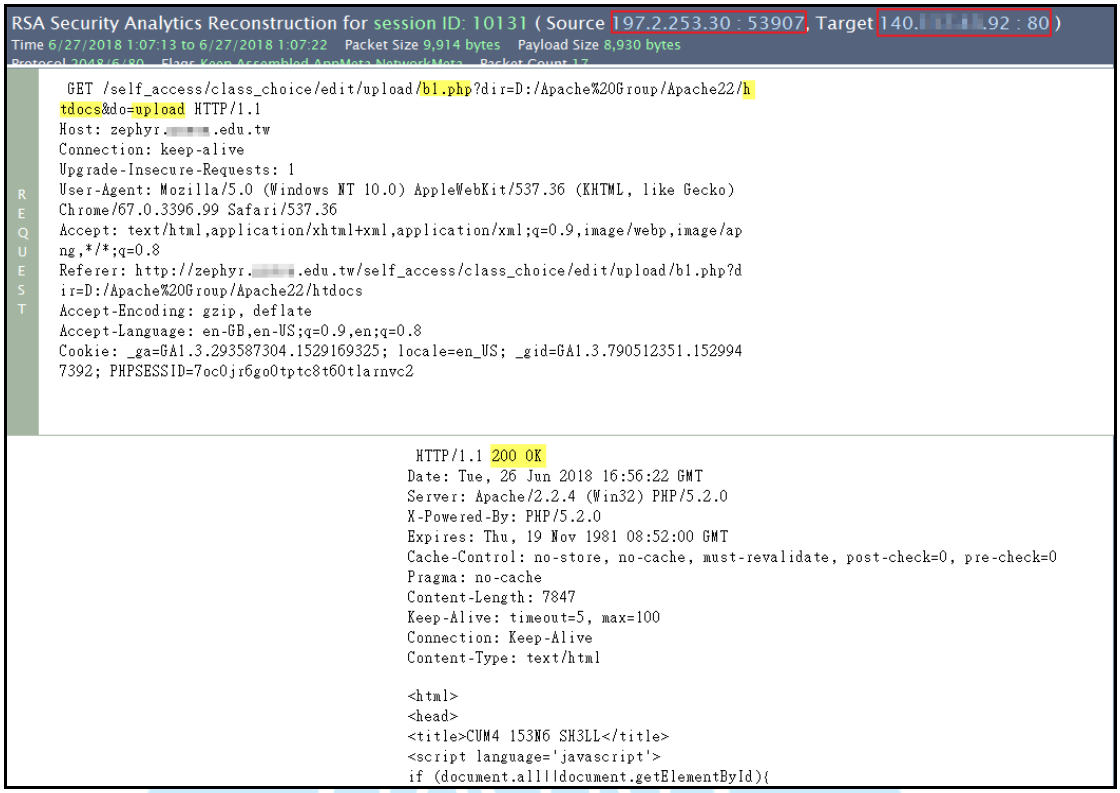
| | | | | | | |
|---|---|---|---|---|---|---|
| CACHED IMAGE config | dir | - | June 21 2018 2:04:26 | 0/0 | drwxrwxrwx | rename \| delete |
| CACHED IMAGE etc_test_register | dir | - | June 21 2018 2:04:26 | 0/0 | drwxrwxrwx | rename \| delete |
| CACHED IMAGE inc | dir | - | June 22 2018 6:51:29 | 0/0 | drwxrwxrwx | rename \| delete |
| CACHED IMAGE phpMyAdmin | dir | - | June 21 2018 2:04:26 | 0/0 | drwxrwxrwx | rename \| delete |
| CACHED IMAGE plugin | dir | - | June 21 2018 2:04:26 | 0/0 | drwxrwxrwx | rename \| delete |

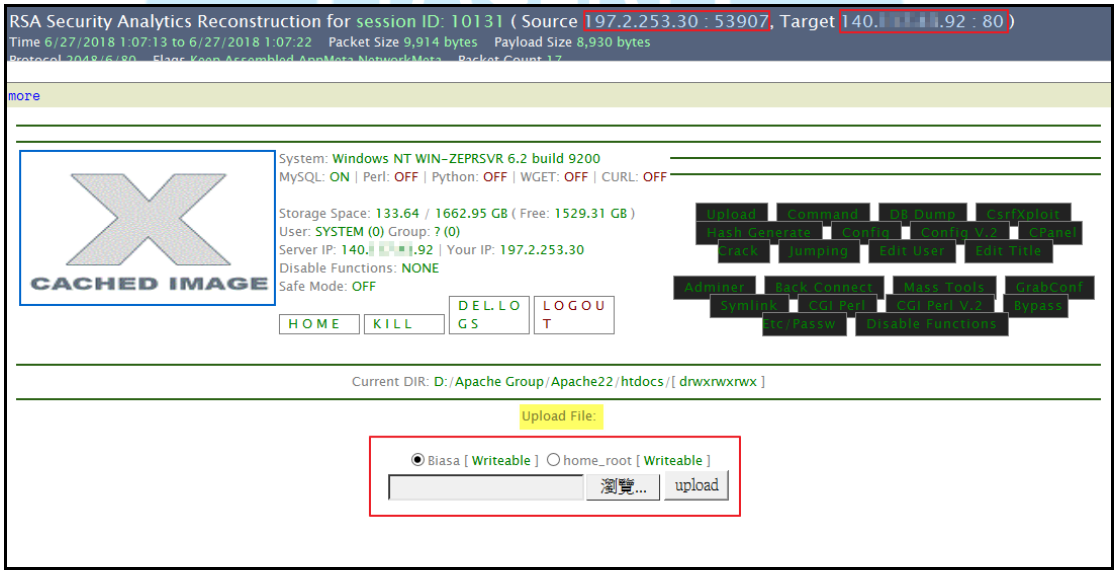
另外，也發現駭客曾對 b1.php、cmd.php、php.ini 與 wso.php 等檔案進行過權限修改。

RSA Security Analytics Reconstruction for session ID: 13445 ( Source 197.2.253.30 : 54683 Target 140.[redacted].92 : 80 )
Time 6/27/2018 1:15:03 to 6/27/2018 1:15:22 Packet Size 112,502 bytes Payload Size 105,596 bytes

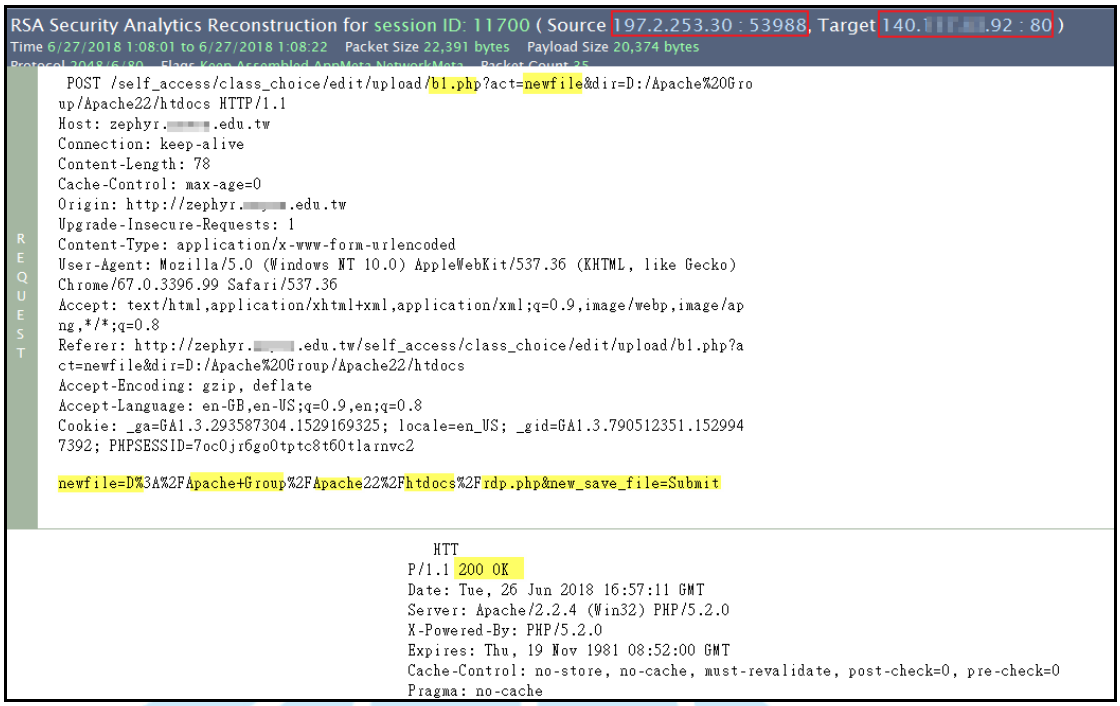
| | | | | | | |
|---|---|---|---|---|---|---|
| CACHED IMAGE b1.php | file | 1.63MB | June 16 2018 5:02:42 | 0/0 | -rw-rw-rw- | edit \| rename \| delete \| download |
| CACHED IMAGE cmd.php | file | 8.108KB | June 17 2018 1:11:51 | 0/0 | -rw-rw-rw- | edit \| rename \| delete \| download |
| CACHED IMAGE php.ini | file | 0.041KB | June 27 2018 12:54:13 | 0/0 | -rw-rw-rw- | edit \| rename \| delete \| download |
| CACHED IMAGE wso.php | file | 321.104KB | June 16 2018 5:58:10 | 0/0 | -rw-rw-rw- | edit \| rename \| delete \| download |

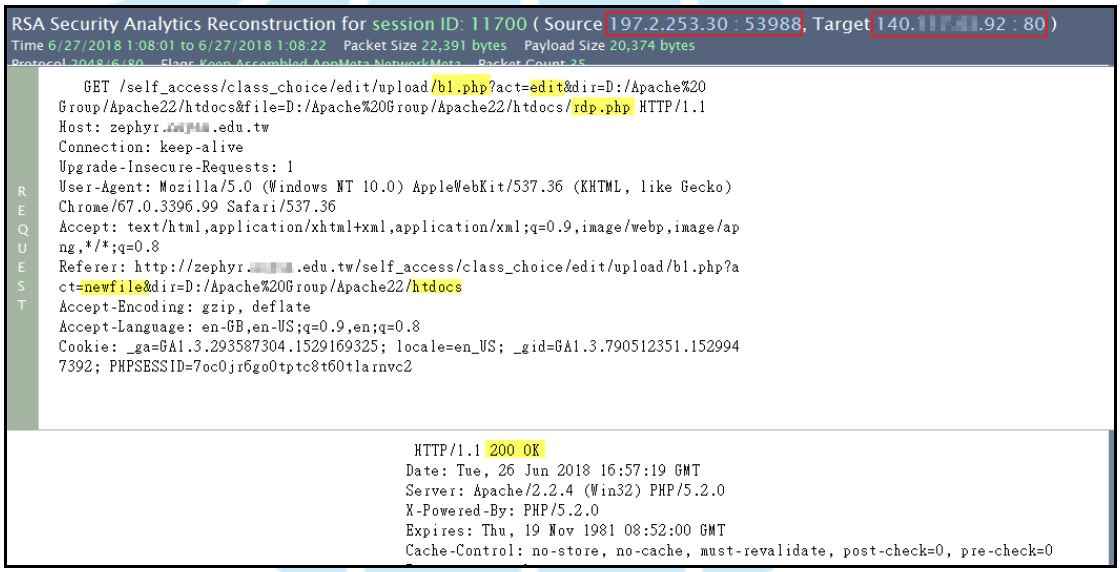
(3)駭客透過 b1.php 的 WebShell 後門程式可以執行 upload 的指令到受害主機內。

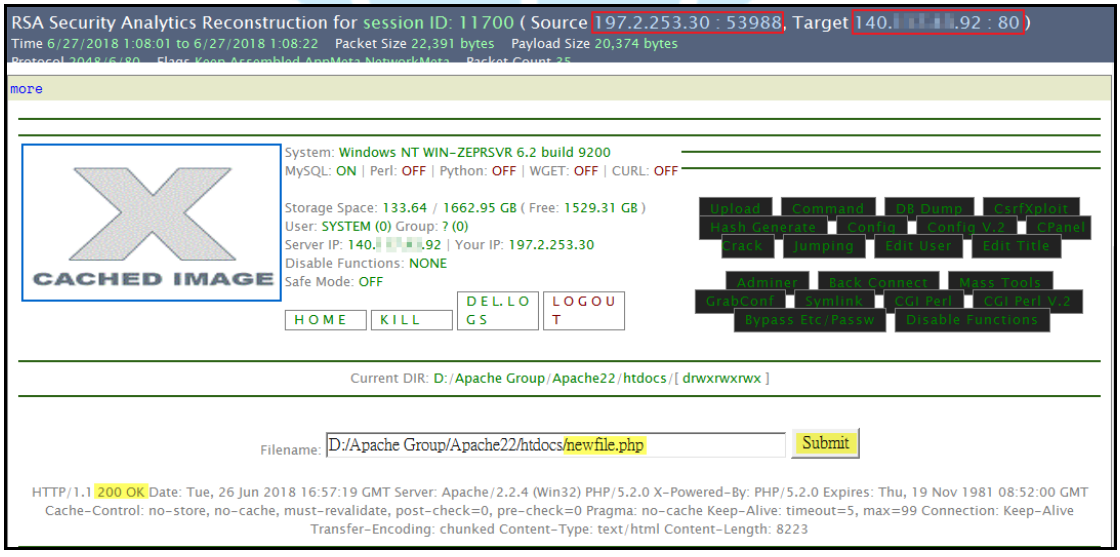


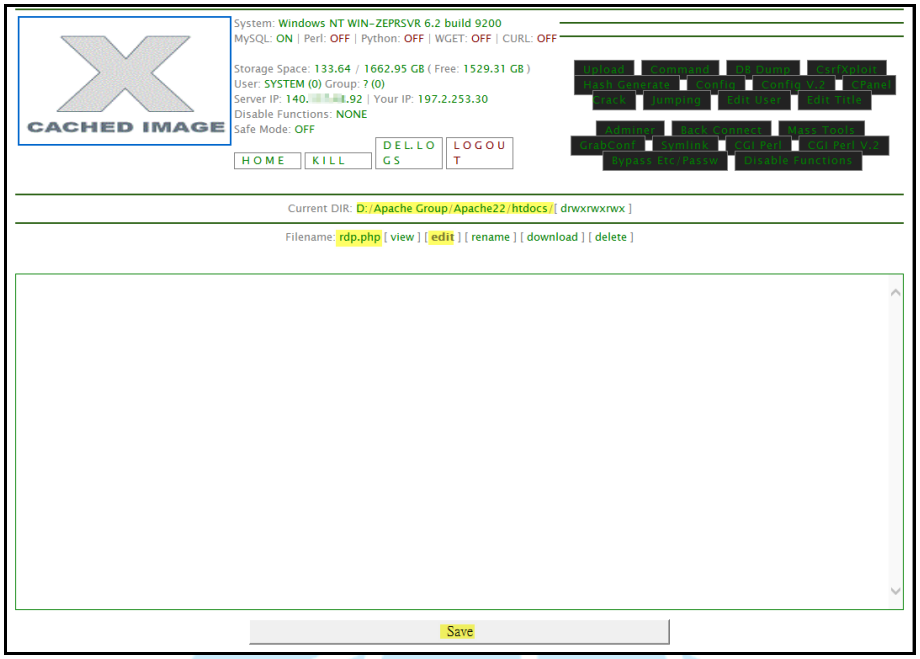




(4)駭客透過 b1.php 可新增一個檔案 rdp.php 到 htdocs 內，並且編輯它。

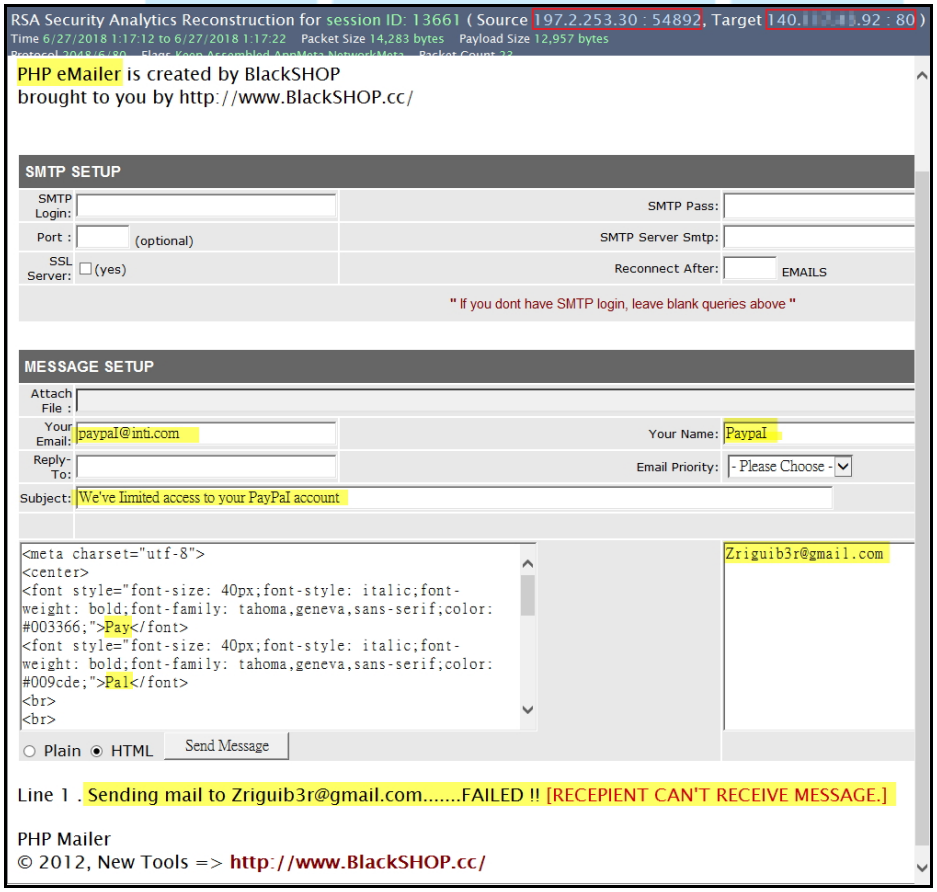

RSA Security Analytics Reconstruction for session ID: 11700 ( Source 197.2.253.30 : 53988, Target 140.[redacted].92 : 80 )
Time 6/27/2018 1:08:01 to 6/27/2018 1:08:22 Packet Size 22,391 bytes Payload Size 20,374 bytes
REQUEST
POST /self_access/class_choice/edit/upload/b1.php?act=newfile&dir=D:/Apache%20Gro
up/Apache22/htdocs HTTP/1.1
Host: zephyr.[redacted].edu.tw
Connection: keep-alive
Content-Length: 78
Cache-Control: max-age=0
Origin: http://zephyr.[redacted].edu.tw
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/67.0.3396.99 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://zephyr.[redacted].edu.tw/self_access/class_choice/edit/upload/b1.php?a
ct=newfile&dir=D:/Apache%20Group/Apache22/htdocs
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: _ga=GA1.3.293587304.1529169325; locale=en_US; _gid=GA1.3.790512351.152994
7392; PHPSESSID=7oc0jr6go0tptc8t60tlarnvc2
newfile=D%3A%2FApache+Group%2FApache22%2Fhtdocs%2Frdp.php&new_save_file=Submit
HTTP/1.1 200 OK
Date: Tue, 26 Jun 2018 16:57:11 GMT
Server: Apache/2.2.4 (Win32) PHP/5.2.0
X-Powered-By: PHP/5.2.0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache


RSA Security Analytics Reconstruction for session ID: 11700 ( Source 197.2.253.30 : 53988, Target 140.[redacted].92 : 80 )
Time 6/27/2018 1:08:01 to 6/27/2018 1:08:22 Packet Size 22,391 bytes Payload Size 20,374 bytes
REQUEST
GET /self_access/class_choice/edit/upload/b1.php?act=edit&dir=D:/Apache%20
Group/Apache22/htdocs&file=D:/Apache%20Group/Apache22/htdocs/rdp.php HTTP/1.1
Host: zephyr.[redacted].edu.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/67.0.3396.99 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://zephyr.[redacted].edu.tw/self_access/class_choice/edit/upload/b1.php?a
ct=newfile&dir=D:/Apache%20Group/Apache22/htdocs
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: _ga=GA1.3.293587304.1529169325; locale=en_US; _gid=GA1.3.790512351.152994
7392; PHPSESSID=7oc0jr6go0tptc8t60tlarnvc2
HTTP/1.1 200 OK
Date: Tue, 26 Jun 2018 16:57:19 GMT
Server: Apache/2.2.4 (Win32) PHP/5.2.0
X-Powered-By: PHP/5.2.0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0


RSA Security Analytics Reconstruction for session ID: 11700 ( Source 197.2.253.30 : 53988, Target 140.[redacted].92 : 80 )
Time 6/27/2018 1:08:01 to 6/27/2018 1:08:22 Packet Size 22,391 bytes Payload Size 20,374 bytes
more
CACHED IMAGE
System: Windows NT WIN-ZEPRSVR 6.2 build 9200
MySQL: ON | Perl: OFF | Python: OFF | WGET: OFF | CURL: OFF
Storage Space: 133.64 / 1662.95 GB ( Free: 1529.31 GB )
User: SYSTEM (0) Group: ? (0)
Server IP: 140.[redacted].92 | Your IP: 197.2.253.30
Disable Functions: NONE
Safe Mode: OFF
HOME
KILL
DEL.LOGS
LOGOUT
Upload
Command
DB Dump
CsrfXploit
Hash Generate
Config
Config V.2
CPanel
Crack
Jumping
Edit User
Edit Title
Adminer
Back Connect
Mass Tools
GrabConf
Symlink
CGI Perl
CGI Perl V.2
Bypass Etc/Passw
Disable Functions
Current DIR: D:/Apache Group/Apache22/htdocs/[ drwxrwxrwx ]
Filename: D:/Apache Group/Apache22/htdocs/newfile.php
Submit
HTTP/1.1 200 OK Date: Tue, 26 Jun 2018 16:57:19 GMT Server: Apache/2.2.4 (Win32) PHP/5.2.0 X-Powered-By: PHP/5.2.0 Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=99 Connection: Keep-Alive
Transfer-Encoding: chunked Content-Type: text/html Content-Length: 8223




(5)駭客透過 rdp.php 執行系統自動寄信功能，在 rdp.php 內容可以看到一個由 BlackSHOP 所製作的 PHP eMailer 寄信器，而且駭客試著以 paypaI@inti.com 之名義對 Zriguib3r@gmail.com 寄出一個主旨為「We’ve limited access to your PayPal account」之信件，但未成功寄出。



從信件內容可以看出駭客告訴對方帳戶即將在 24 小時內過期，請對方點選連結驗證帳戶。該連結 http://we-loading-please-wait.blogspot.com 為可疑網址。

```
<br>
<div style="border: 1px solid #efe9e9;width: 650px;text-
align: center;padding: 2px;">
<h4>
<font color="#019be1">Notice of Policy Updates</font></h4>
paypal Client,
<br>
<br>
Your account will be suspended after 24 hours.
<br>
```

```
<br>
Please update your information promptly
<br>
<h5>
<a href="javascript:alert('This%20link%20navigates%
20to:\n\nhttp://we-loading-please-wait.blogspot.com/?
m=0');">Click Here To Verfie your Account</a>
</h5>
</div>
<br>
```

(6)駭客透過 wso.php 上傳 Stupidc0de.php 檔，Stupidc0de.php 為一個後門程式，駭客可以透過它進行 RDP 遠端連線。

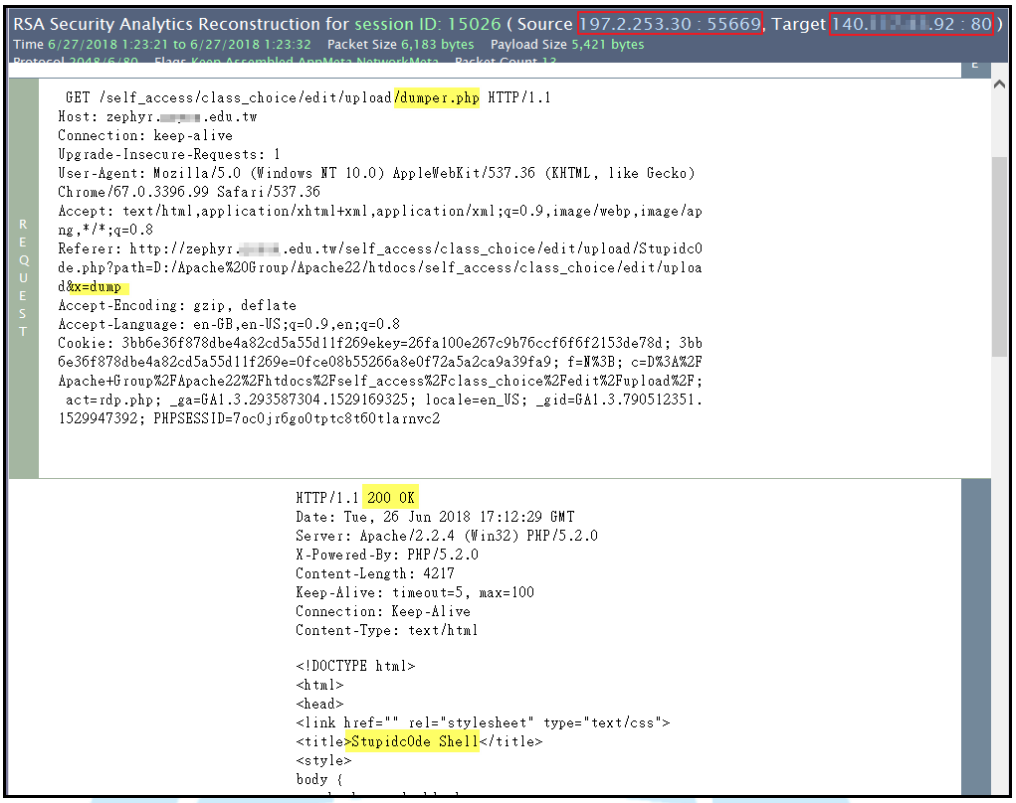
RSA Security Analytics Reconstruction for session ID: 14892 ( Source 197.2.253.30 : 55505, Target 140.[redacted].92 : 80 )
Time 6/27/2018 1:21:54 to 6/27/2018 1:22:07 Packet Size 437,940 bytes Payload Size 407,834 bytes

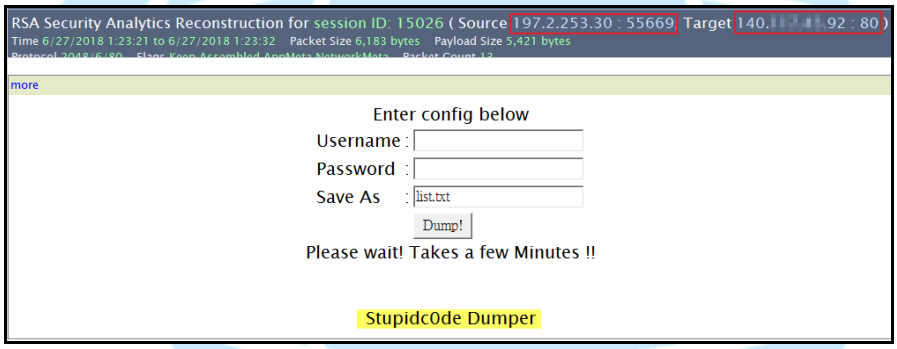
REQUEST

```
POST /self_access/class_choice/edit/upload/wso.php HTTP/1.1
Host: zephyr.[redacted].edu.tw
Connection: keep-alive
Content-Length: 353951
Cache-Control: max-age=0
Origin: http://zephyr.[redacted].edu.tw
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymRQhXhjaQyka4Hv
6
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/67.0.3396.99 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://zephyr.[redacted].edu.tw/self_access/class_choice/edit/upload/wso.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: 3bb6e36f878dbe4a82cd5a55d11f269ekey=26fa100e267c9b76ccf6f6f2153de78d; 3bb
6e36f878dbe4a82cd5a55d11f269e=0fce08b55266a8e0f72a5a2ca9a39fa9; f=N%3B; c=D%3A%2F
Apache+Group%2FApache22%2Fhtdocs%2Fself_access%2Fclass_choice%2Fedit%2Fupload%2F;
act=rdp.php; _ga=GA1.3.293587304.1529169325; locale=en_US; _gid=GA1.3.790512351.
1529947392; PHPSESSID=7oc0jr6go0tptc8t60tlarnvc2

------WebKitFormBoundarymRQhXhjaQyka4Hv6
Content-Disposition: form-data; name="a"

FilesMan
------WebKitFormBoundarymRQhXhjaQyka4Hv6
Content-Disposition: form-data; name="c"

D:/Apache Group/Apache22/htdocs/self_access/class_choice/edit/upload/
------WebKitFormBoundarymRQhXhjaQyka4Hv6
Content-Disposition: form-data; name="p1"

uploadFile
------WebKitFormBoundarymRQhXhjaQyka4Hv6
Content-Disposition: form-data; name="ne"


------WebKitFormBoundarymRQhXhjaQyka4Hv6
Content-Disposition: form-data; name="charset"

UTF-8
------WebKitFormBoundarymRQhXhjaQyka4Hv6
Content-Disposition: form-data; name="f[]"; filename="Stupidc0de.php"
Content-Type: application/octet-stream

<?php
/*
```

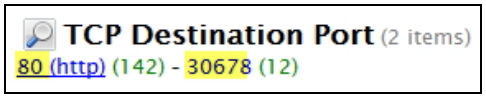

(7)駭客藉著 Stupidc0de.php，可抓取受害主機內的密碼內容。

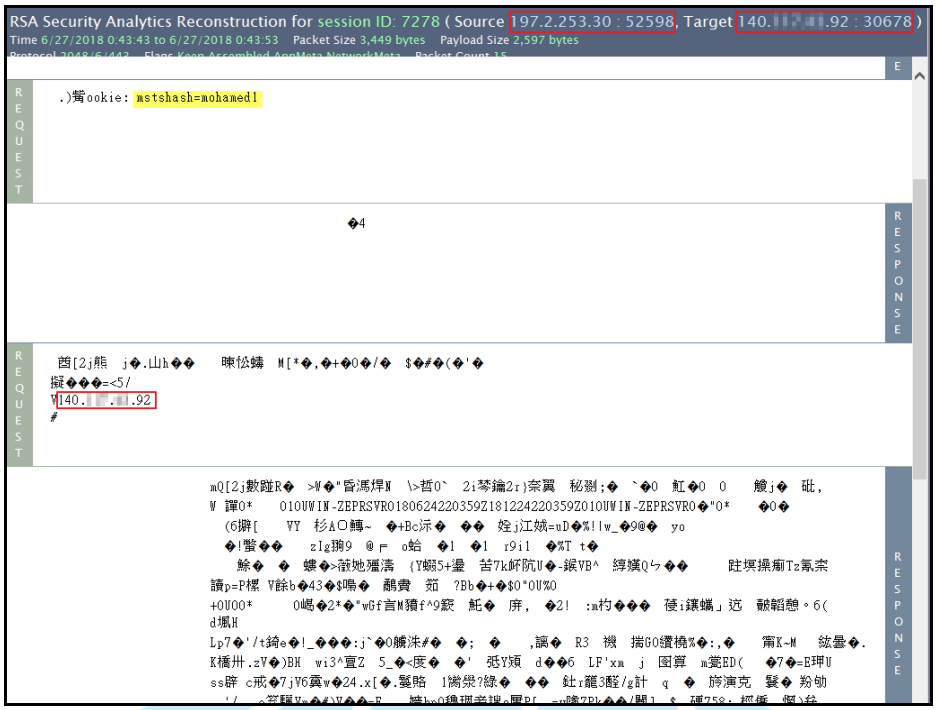

(8)駭客使用 Stupidc0de.php 的 Dumper 功能，透過 dumper.php 將 Username 與 Password 存入 list.txt 內。



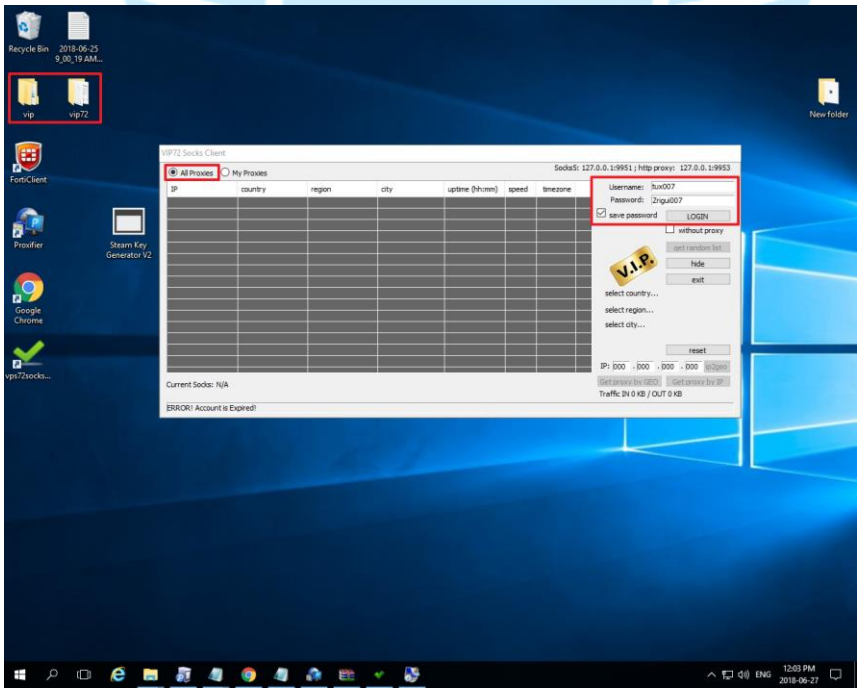

11. 觀察封包連線情形可以得知該突尼西亞駭客 IP 連線受害主機的 80 port 與 30678 port 多次，而從封包內容可以看到駭客以 30678 port 登入帳戶 mohamed1。

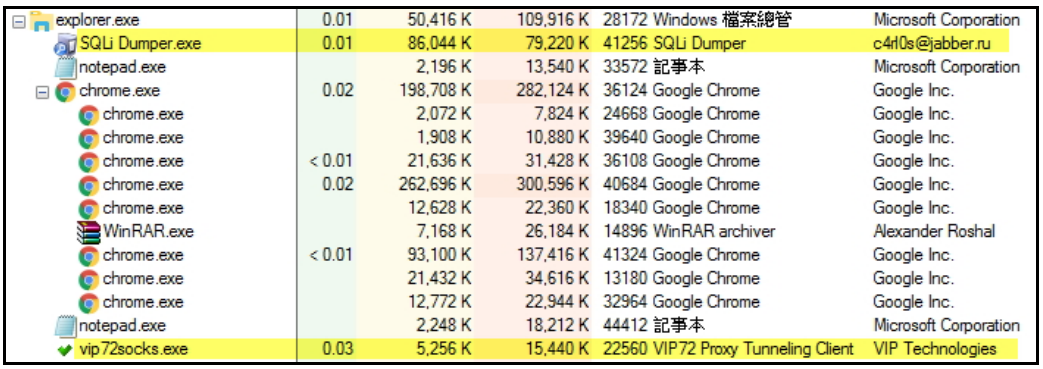





12. 在檢測期間因發現駭客仍遠端連線登入受害主機桌面，並在具有系統管理者權限的使用者帳戶 mohamed1 下執行一些程式。待駭客離線後，登入其 mohamed1 帳戶桌面，發現駭客將受害主機當作練習駭客工具的測試機。

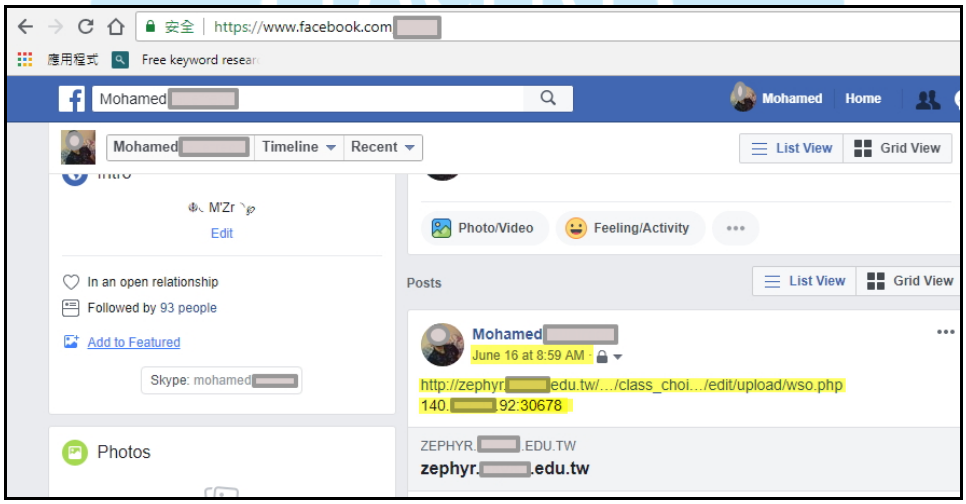
（1） 從桌面看到駭客正在使用匿名的 proxy 工具 vip72 socks client 與執行一些程式，如 SQLi Dumper.exe，而 vip72 socks client.exe 經 virustotal 檢測惡意比例為 15/67。



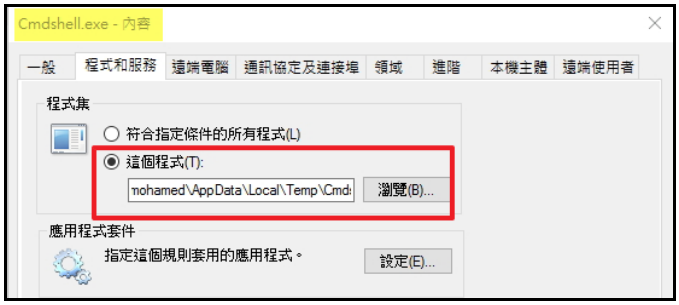


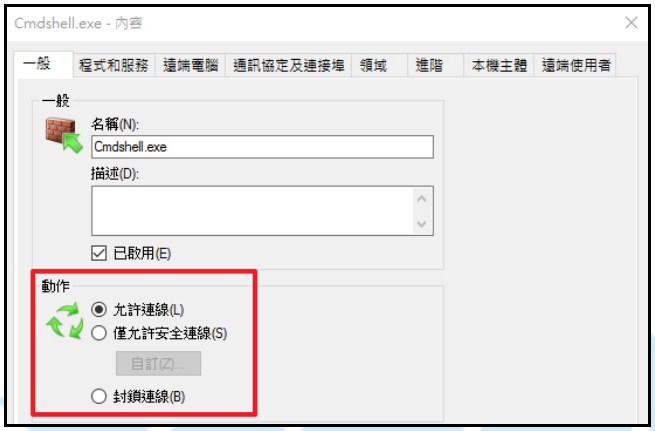
| | | | | | |
|---|---|---|---|---|---|
| explorer.exe | 0.01 | 50,416 K | 109,916 K | 28172 Windows 檔案總管 | Microsoft Corporation |
| SQLi Dumper.exe | 0.01 | 86,044 K | 79,220 K | 41256 SQLi Dumper | c4rl0s@jabber.ru |
| notepad.exe | | 2,196 K | 13,540 K | 33572 記事本 | Microsoft Corporation |
| chrome.exe | 0.02 | 198,708 K | 282,124 K | 36124 Google Chrome | Google Inc. |
| chrome.exe | | 2,072 K | 7,824 K | 24668 Google Chrome | Google Inc. |
| chrome.exe | | 1,908 K | 10,880 K | 39640 Google Chrome | Google Inc. |
| chrome.exe | < 0.01 | 21,636 K | 31,428 K | 36108 Google Chrome | Google Inc. |
| chrome.exe | 0.02 | 262,696 K | 300,596 K | 40684 Google Chrome | Google Inc. |
| chrome.exe | | 12,628 K | 22,360 K | 18340 Google Chrome | Google Inc. |
| WinRAR.exe | | 7,168 K | 26,184 K | 14896 WinRAR archiver | Alexander Roshal |
| chrome.exe | < 0.01 | 93,100 K | 137,416 K | 41324 Google Chrome | Google Inc. |
| chrome.exe | | 21,432 K | 34,616 K | 13180 Google Chrome | Google Inc. |
| chrome.exe | | 12,772 K | 22,944 K | 32964 Google Chrome | Google Inc. |
| notepad.exe | | 2,248 K | 18,212 K | 44412 記事本 | Microsoft Corporation |
| vip72socks.exe | 0.03 | 5,256 K | 15,440 K | 22560 VIP72 Proxy Tunneling Client | VIP Technologies |


(2) 發現駭客開啟個人 Facebook 未關閉，並且將此受害主機的網站漏洞資訊與遠端連線 port 張貼於 Facebook 上，而且與網友私訊討論如何遠端登入受害主機。

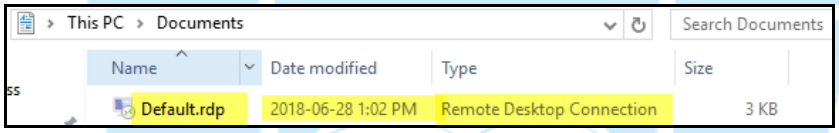



(3)在 C:\使用者\mohamed\AppData\Local\Temp 內，有一個程式 Cmdshell.exe 在執行，而且設定為允許連線，猜測駭客可能透過此程式從遠端連入下達 cmd 指令。

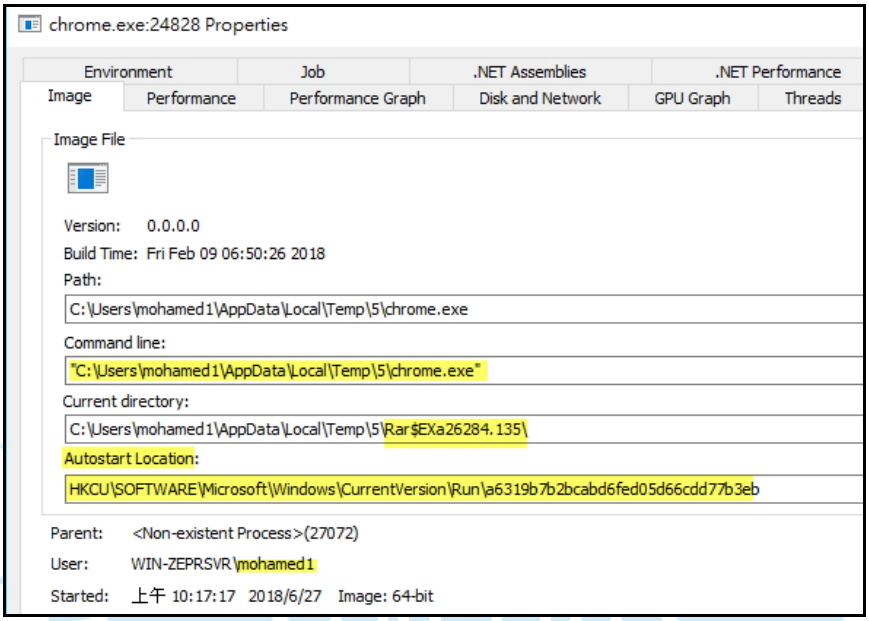


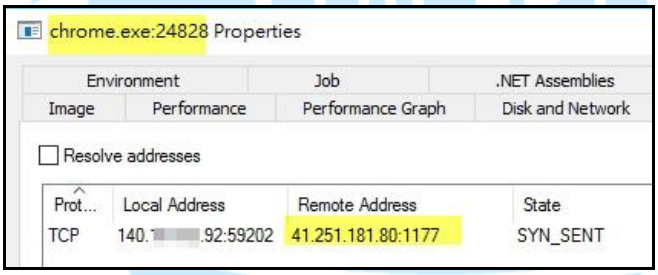




(4)在 Documents 資料夾內發現 Default.rdp 遠端桌面連線預設檔，此為該主機曾被遠端連線的痕跡，又從事件檢視器得知，該主機曾被 IP:197.2.253.30 多次遠端連線登入。



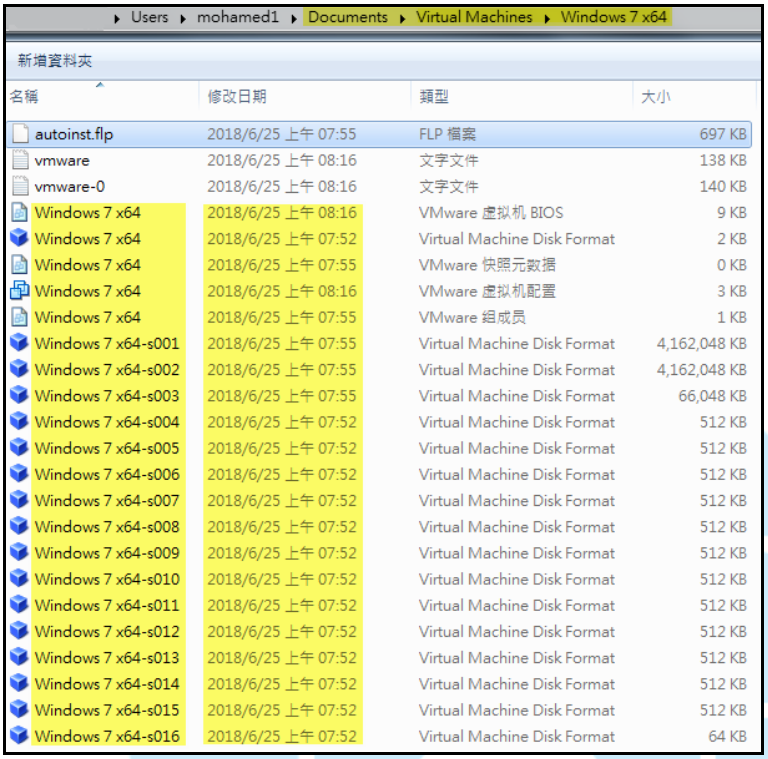

(5)檢視背景程式執行狀況，發現有一個異常的 Chrome.exe 正在執行，而且連線南非 IP:41.251.181.80:1177，從屬性內容可得知此非正常 Chrome 程式，因為此 Chrome.exe 所在位置在 Temp 資料夾內，而且在重新開機後會自行啟動。

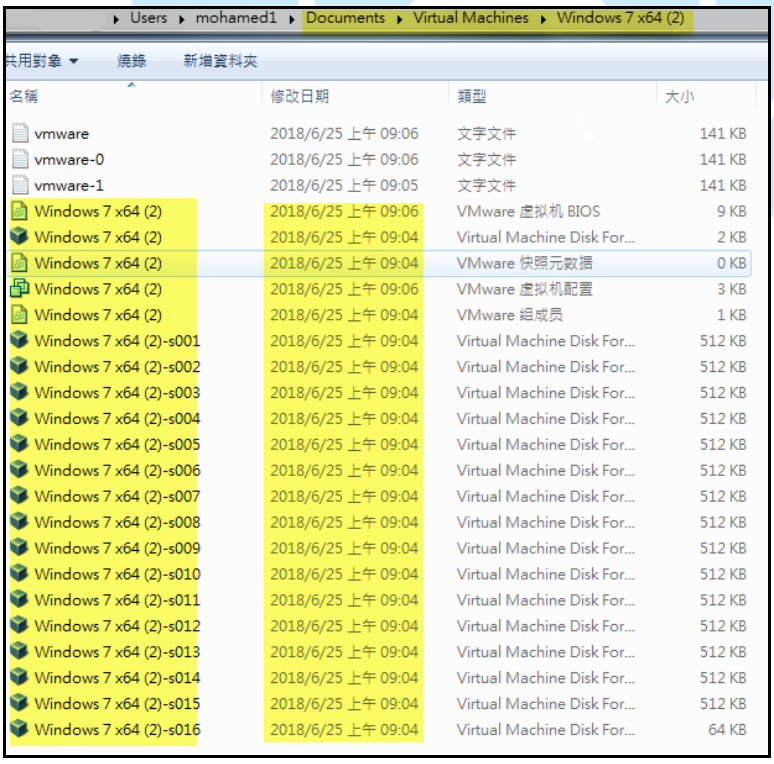


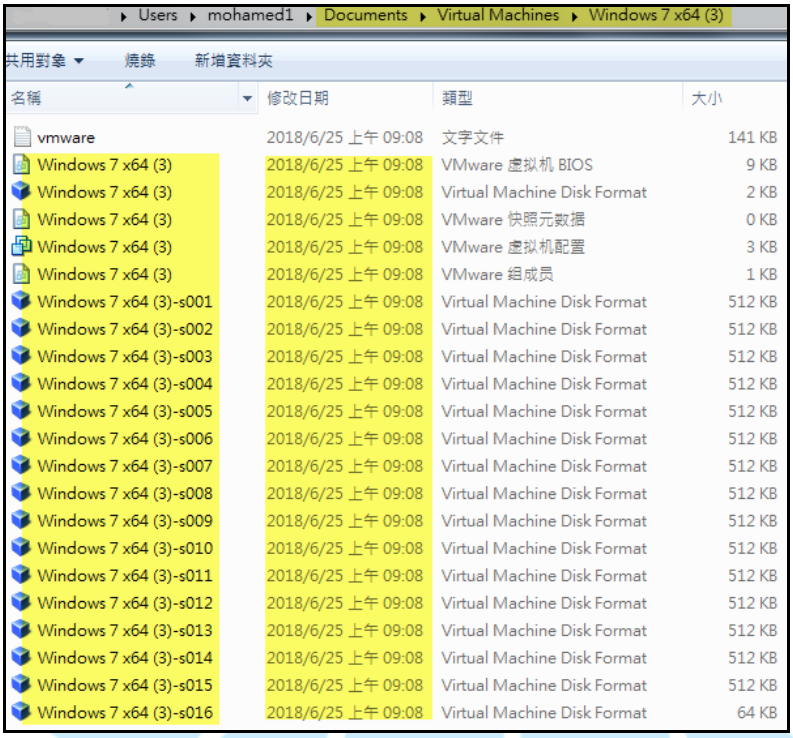




(6)檢視下載資料夾，發現駭客在入侵主機期間，下載 VPN 程式、VMware workstation 安裝程式、Steam 金鑰產生器、mail.txt、Win 7 安裝程式與 vip72 執行檔，可見駭客將此主機視為練習各類程式的練習場。

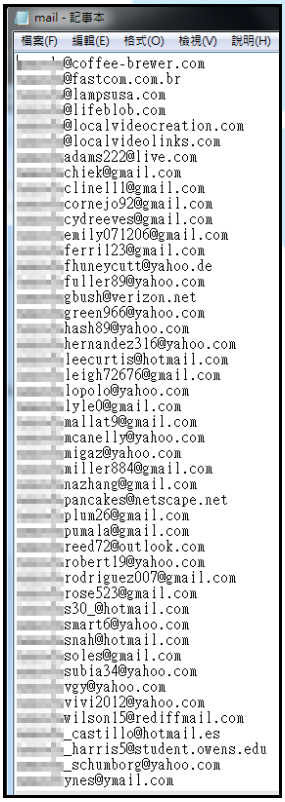
(7)因發現駭客下載 VMware Workstation 12 與 Windows 7，推測駭客應該有安裝 Windows 7 的虛擬機於受害主機內。在 Documents/Virtual Machines 資料夾內，發現三個資料夾內有 Windows 7 的 VM 虛擬機，而且每個都快照 16 次，推測駭客可能利用這些虛擬機進行某種測試，並儲存測試結果。

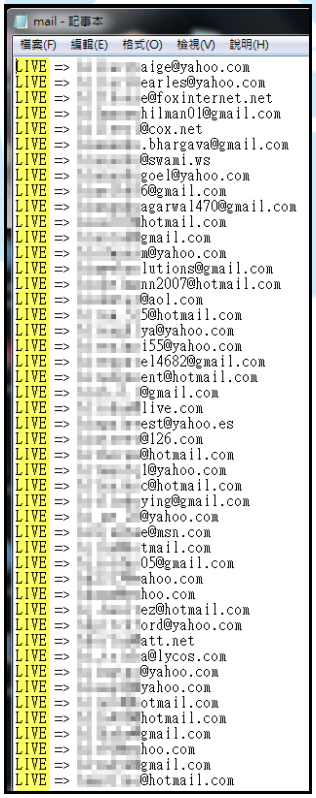




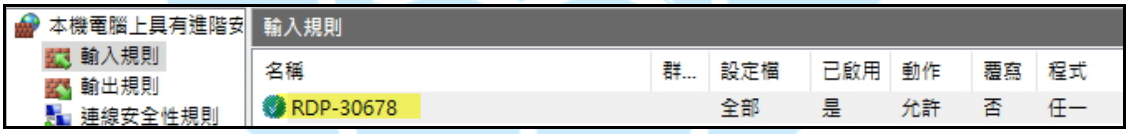

(8)將在下載資料夾內的 mail.txt 文字檔開啟後，發現裡面有許多 E-mail 帳號，又在使用者桌面資料夾內發現一個 mail.txt 文字檔，開啟後發現裡面一樣有許多 E-mail 帳號，但是每個帳號有 LIVE 用字在 E-mail 帳號前，推測此為駭客測試 E-mail 帳號是否仍被使用的存檔資料。

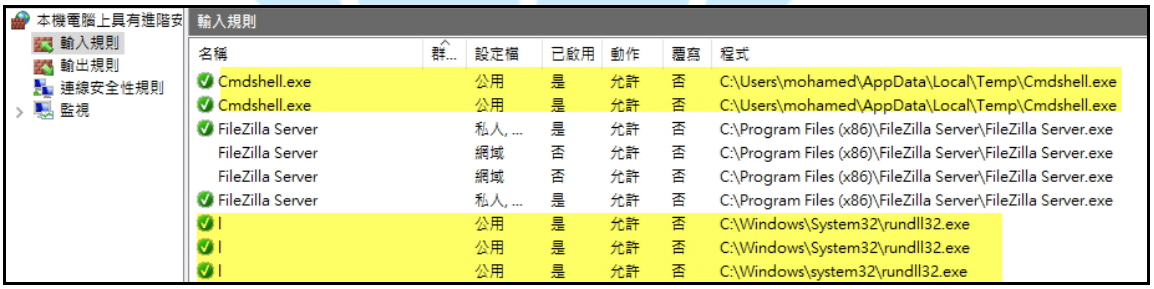


(9)從 Chrome 之密碼管理設定中，發現駭客存入一組帳號與密碼，而使用者名稱 zriguib3r@gmail.com 與封包所側錄到的 PHP E-mailer 自動寄信器之收信者 E-mail 相同，可見駭客當時正在自我測試是否可以將信件成功寄出。

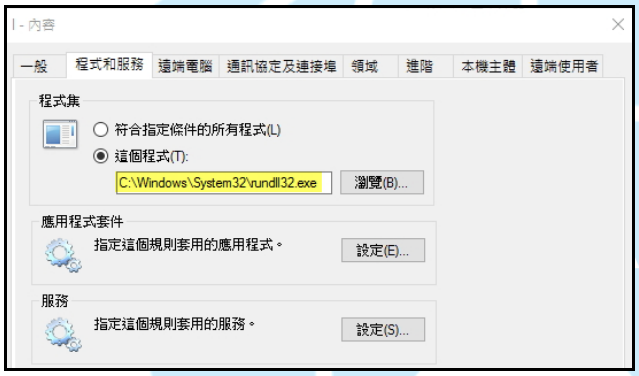

13. 檢視受害主機 port 開啟狀況，發現除了系統管理者遠端連線用之 RDP-30678 輸入規則(開啟 30678port)外，另有不明來源的輸入規則 Cmdshell.exe 與 I 兩規則，以及其他遠端桌面的相關輸入規則是開啟狀態，提供駭客很多入侵主機的管道。



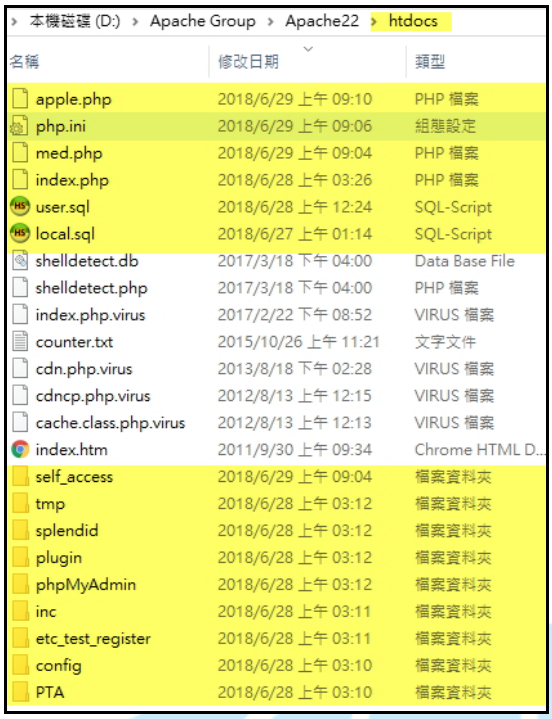




14. 檢視背景程式發現除了挖礦程式 gAF90.tmp.exe 外，還有許多 rundll32.exe 在執行著，而且發現防火牆輸入規則 I 所開啟的 port 與此程式 rundll32.exe 有關。

| Process Name | Process ID | Protocol | Local P... | Local Address | Remote ... | R | Remote Address |
|---|---|---|---|---|---|---|---|
| Unknown | 0 | TCP | 31622 | 140. 92 | 60271 | | 180.254.208.48 |
| gAF90.tmp.exe | 8168 | TCP | 53556 | 140. 92 | 5555 | | 217.147.169.170 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 21287 | | 180.245.186.255 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 52909 | | 178.54.48.38 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 51731 | | 105.128.199.42 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 60960 | | 41.34.35.234 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 22535 | | 105.105.41.73 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 56999 | | 105.158.227.164 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 49254 | | 171.239.186.53 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 55130 | | 94.128.130.181 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 50102 | | 79.106.35.108 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 51308 | | 154.70.17.145 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 56305 | | 79.17.7.44 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 62150 | | 42.110.138.47 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 63476 | | 109.108.83.72 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 32516 | | 43.249.235.181 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 11936 | | 109.163.162.168 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 7641 | | 106.206.47.111 |
| rundll32.exe | 7532 | TCP | 31622 | 140. 92 | 53662 | | 157.32.58.247 |

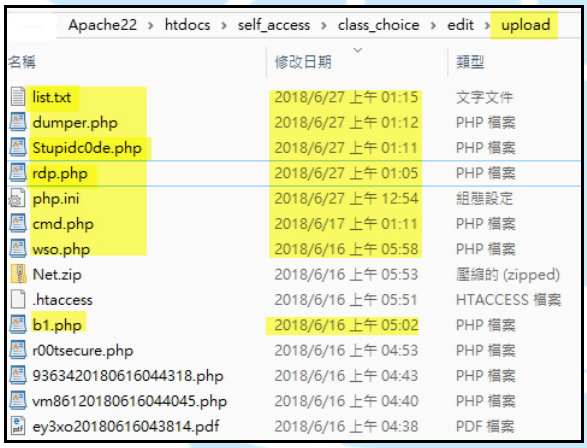



15. 查看網站 Apache Server 所在資料夾，發現有許多檔案與資料夾被修改過，可見駭客透過 upload 資料夾入侵後完全掌控受害主機，而 upload 資料夾內的 list.txt 疑似為駭客所收集的學員的 E-mail 帳號之檔案。



本機磁碟 (D:) › Apache Group › Apache22 › htdocs

| 名稱 | 修改日期 | 類型 |
|---|---|---|
| apple.php | 2018/6/29 上午 09:10 | PHP 檔案 |
| php.ini | 2018/6/29 上午 09:06 | 組態設定 |
| med.php | 2018/6/29 上午 09:04 | PHP 檔案 |
| index.php | 2018/6/28 上午 03:26 | PHP 檔案 |
| user.sql | 2018/6/28 上午 12:24 | SQL-Script |
| local.sql | 2018/6/27 上午 01:14 | SQL-Script |
| shelldetect.db | 2017/3/18 下午 04:00 | Data Base File |
| shelldetect.php | 2017/3/18 下午 04:00 | PHP 檔案 |
| index.php.virus | 2017/2/22 下午 08:52 | VIRUS 檔案 |
| counter.txt | 2015/10/26 上午 11:21 | 文字文件 |
| cdn.php.virus | 2013/8/18 下午 02:28 | VIRUS 檔案 |
| cdncp.php.virus | 2012/8/13 上午 12:15 | VIRUS 檔案 |
| cache.class.php.virus | 2012/8/13 上午 12:13 | VIRUS 檔案 |
| index.htm | 2011/9/30 上午 09:34 | Chrome HTML D... |
| self_access | 2018/6/29 上午 09:04 | 檔案資料夾 |
| tmp | 2018/6/28 上午 03:12 | 檔案資料夾 |
| splendid | 2018/6/28 上午 03:12 | 檔案資料夾 |
| plugin | 2018/6/28 上午 03:12 | 檔案資料夾 |
| phpMyAdmin | 2018/6/28 上午 03:12 | 檔案資料夾 |
| inc | 2018/6/28 上午 03:11 | 檔案資料夾 |
| etc_test_register | 2018/6/28 上午 03:11 | 檔案資料夾 |
| config | 2018/6/28 上午 03:10 | 檔案資料夾 |
| PTA | 2018/6/28 上午 03:10 | 檔案資料夾 |

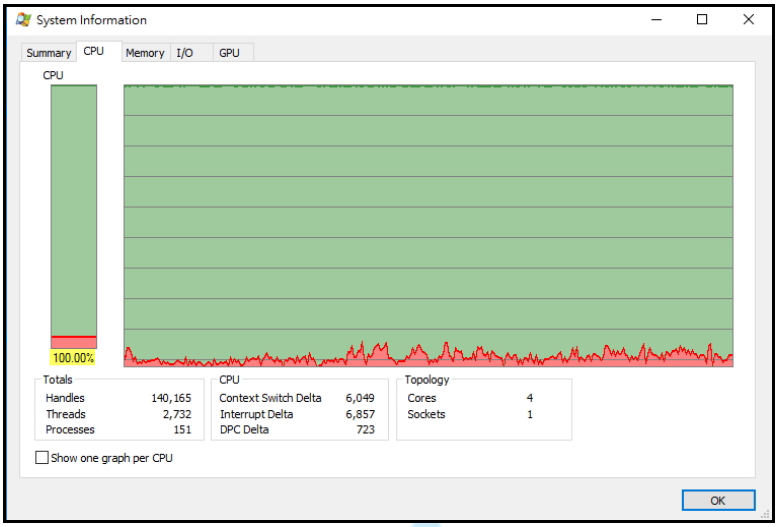


Apache22 › htdocs › self_access › class_choice › edit › upload

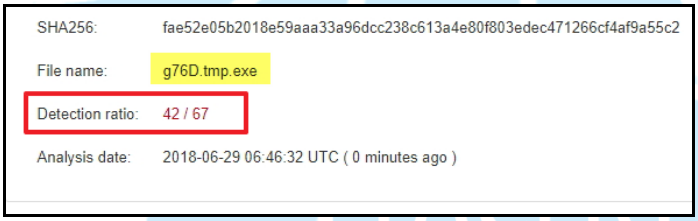
| 名稱 | 修改日期 | 類型 |
|---|---|---|
| list.txt | 2018/6/27 上午 01:15 | 文字文件 |
| dumper.php | 2018/6/27 上午 01:12 | PHP 檔案 |
| Stupidc0de.php | 2018/6/27 上午 01:11 | PHP 檔案 |
| rdp.php | 2018/6/27 上午 01:05 | PHP 檔案 |
| php.ini | 2018/6/27 上午 12:54 | 組態設定 |
| cmd.php | 2018/6/17 上午 01:11 | PHP 檔案 |
| wso.php | 2018/6/16 上午 05:58 | PHP 檔案 |
| Net.zip | 2018/6/16 上午 05:53 | 壓縮的 (zipped) |
| .htaccess | 2018/6/16 上午 05:51 | HTACCESS 檔案 |
| b1.php | 2018/6/16 上午 05:02 | PHP 檔案 |
| r00tsecure.php | 2018/6/16 上午 04:53 | PHP 檔案 |
| 9363420180616044318.php | 2018/6/16 上午 04:43 | PHP 檔案 |
| vm86120180616044045.php | 2018/6/16 上午 04:40 | PHP 檔案 |
| ey3xo20180616043814.pdf | 2018/6/16 上午 04:38 | PDF 檔案 |

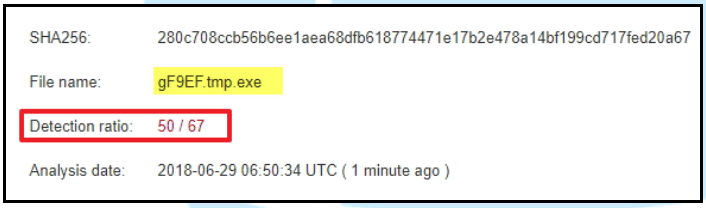
16. 在檢測期間陸續發現檔名相似的.tmp.exe 檔執行挖礦程式，如 g76D.tmp.exe 與 gF9EF.tmp.exe，經 Virustotal 檢測惡意比例分別為 42/67 與 50/67，也發現 notepad.exe 正在連線礦池執行挖礦。

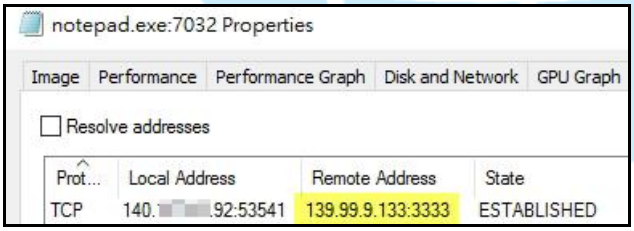
| Added On | Process Name | Process ID | Protoc... | Local P... | Local Address | Remot... | Remote Address | State |
|---|---|---|---|---|---|---|---|---|
| 2018/6/29 下午 02:29:02 | explorer.exe | 6396 | TCP | 51826 | 140.[redacted].92 | 443 | 52.230.80.159 | Established |
| 2018/6/29 下午 02:29:02 | rundll32.exe | 1892 | TCP | 51937 | 140.[redacted].92 | 39718 | 178.32.26.61 | Established |
| 2018/6/29 下午 02:29:02 | notepad.exe | 7532 | TCP | 51947 | 140.[redacted].92 | 3333 | 139.99.9.133 | Established |
| 2018/6/29 下午 02:29:02 | rundll32.exe | 1892 | TCP | 52160 | 140.[redacted].92 | 8685 | 111.118.247.44 | Established |
| 2018/6/29 下午 02:29:02 | chrome.exe | 12488 | TCP | 52336 | 140.[redacted].92 | 443 | 157.240.15.16 | Established |
| 2018/6/29 下午 02:29:02 | g76D.tmp.exe | 5708 | TCP | 52520 | 140.[redacted].92 | 5555 | 217.147.169.170 | Established |
| 2018/6/29 下午 02:29:02 | rundll32.exe | 1892 | TCP | 59330 | 140.[redacted].92 | 46240 | 41.159.135.3 | Established |

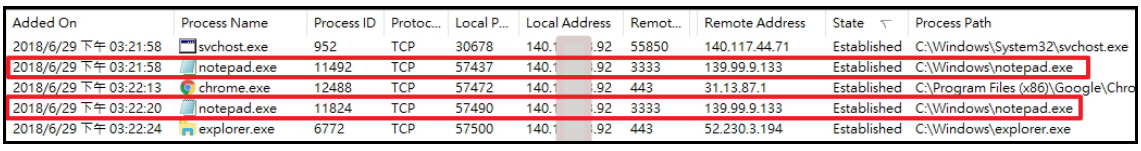




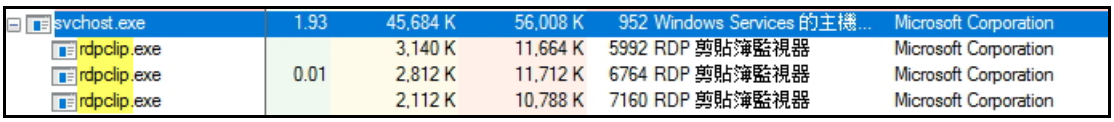


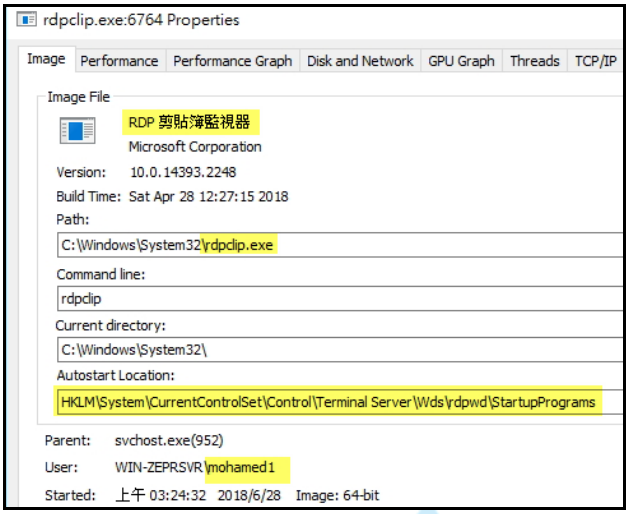



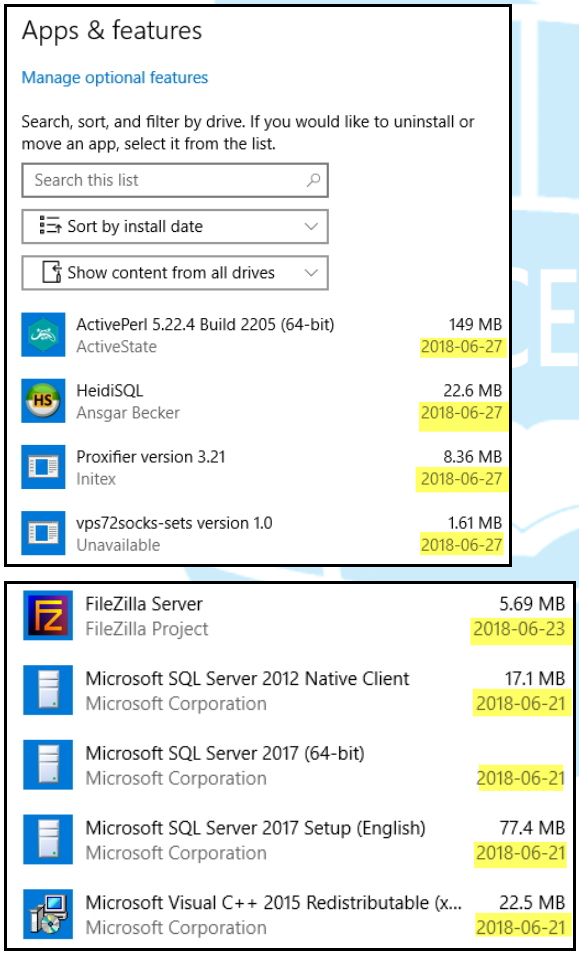




17. 在背景程式中，發現 rdpclip.exe 正在執行，表示遠端桌面連線使用中，而且重新開機時會自動啟用它，提供駭客任何時候都可以從遠端連線。

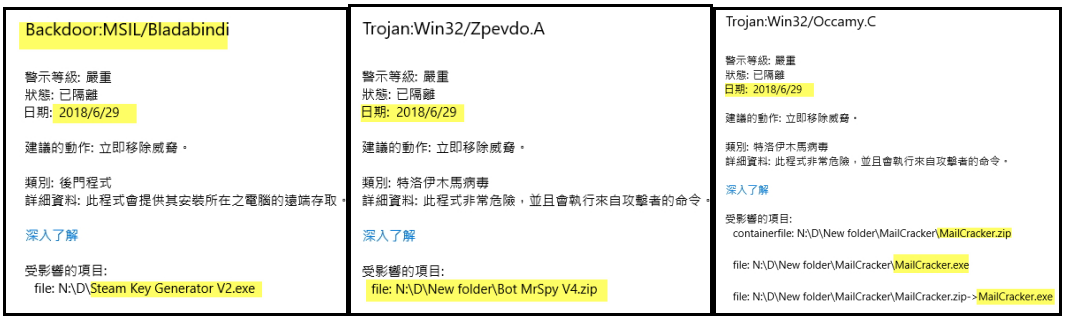





18. 檢視主機中軟體安裝情形，發現駭客於入侵期間安裝許多程式於主機內。




19. 因受害主機未安裝任何防毒軟體，因此無法即時偵測到惡意程式的入侵，當管理者將防毒軟體安裝完成後，即偵測出一些惡意程式的存在。




## III. 網路架構圖


1. 上傳 Webshell 後門程式至網站 upload 資料夾進行入侵
2. 透過 Webshell PHP 檔進行多個動作:
   a. 檔案提權。
   b. 遠端桌面連線。
   c. 下載惡意程式到受害主機內安裝。
   d. 竊取學員 E-mail 資訊。
   e. 測試系統自動寄信功能。
   f. 建立系統管理員權限的使用者帳戶。
   g. 執行挖礦程式。
   h. 開啟一些 port。…。
3. 陸續頻繁以 80 port 與 30678 port 連線受害主機進行各式攻擊行動。

## IV.建議與總結

1. 本事件的發生主要是駭客透過受害主機網站的上傳資料功能駭入 upload 資料夾，因該功能未限定上傳的資料類型，因此駭客上傳 Webshell 的 PHP 後門程式。
2. 當駭客駭入後應用這些 PHP 檔案，對受害主機進行檔案提權、上傳程式、執行遠端連線程式、竊取學員 E-mail 帳號、新增使用者帳戶、下載程式測試…，幾乎完全掌握受害主機。
3. 檢視受害主機資安防護措施發現有下列資安漏洞:

   (1)upload 資料夾未設定上傳資料類型。

   (2)未安裝任何防毒軟體，無法察覺主機異樣。

   (3)遠端桌面連線功能完全對外開啟，未限定來源 IP。
4. 針對受害主機的資安防護，建議下列措施:

   (1)安裝防毒軟體與定期掃毒。

   (2)定期檢查主機狀況。

   (3)限制遠端連線來源 IP。

   (4)限制上傳檔案類型。

   (5)關閉非必要開啟的 port。