Threat Hunting

HW02

Name: 劉定睿 ID: M11409313

Date: 2025-09-25

目錄

Investigating the Local Computer

- First of all I ues command: `netstat -ano` to list all of the connection

```
C:\Users\foren>netstat -ano

使用中連線

  協定    本機位址               外部位址               狀態            PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1468
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       5616
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       5616
  TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING       2752
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5588
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       8704
  TCP    0.0.0.0:8834           0.0.0.0:0              LISTENING       7020
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1204
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1028
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       3108
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       3088
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       4928
  TCP    0.0.0.0:49694          0.0.0.0:0              LISTENING       1156
  TCP    127.0.0.1:8053         0.0.0.0:0              LISTENING       3864
  TCP    127.0.0.1:9080         0.0.0.0:0              LISTENING       5228
  TCP    127.0.0.1:22350        0.0.0.0:0              LISTENING       11232
  TCP    127.0.0.1:36167        0.0.0.0:0              LISTENING       15060
  TCP    127.0.0.1:49692        127.0.0.1:49693        ESTABLISHED     7020
  TCP    127.0.0.1:49693        127.0.0.1:49692        ESTABLISHED     7020
  TCP    127.0.0.1:49697        127.0.0.1:49698        ESTABLISHED     7020
  TCP    127.0.0.1:49698        127.0.0.1:49697        ESTABLISHED     7020
  TCP    127.0.0.1:50708        127.0.0.1:55017        ESTABLISHED     23740
  TCP    127.0.0.1:55017        0.0.0.0:0              LISTENING       11612
  TCP    127.0.0.1:55017        127.0.0.1:50708        ESTABLISHED     11612
```

- There's too much log so we nee to filter it by `id=3` .
    - use: `netstat -ano | findstr ESTABLISHED`

```
C:\Users\foren>netstat -ano | findstr ESTABLISHED
  TCP    127.0.0.1:49692        127.0.0.1:49693        ESTABLISHED     7020
  TCP    127.0.0.1:49693        127.0.0.1:49692        ESTABLISHED     7020
  TCP    127.0.0.1:49697        127.0.0.1:49698        ESTABLISHED     7020
  TCP    127.0.0.1:49698        127.0.0.1:49697        ESTABLISHED     7020
  TCP    127.0.0.1:50708        127.0.0.1:55017        ESTABLISHED     23740
  TCP    127.0.0.1:55017        127.0.0.1:50708        ESTABLISHED     11612
  TCP    192.168.1.143:50672    172.166.106.148:443    ESTABLISHED     6016
  TCP    192.168.1.143:50678    91.108.56.122:443      ESTABLISHED     16980
  TCP    192.168.1.143:50680    172.167.2.3:443        ESTABLISHED     4792
  TCP    192.168.1.143:50745    31.13.87.4:443         ESTABLISHED     14908
  TCP    192.168.1.143:50749    31.13.87.53:443        ESTABLISHED     14908
  TCP    192.168.1.143:50750    31.13.87.1:443         ESTABLISHED     14908
  TCP    192.168.1.143:50757    44.230.16.251:443      ESTABLISHED     14908
  TCP    192.168.1.143:50758    175.97.131.54:443      ESTABLISHED     14908
  TCP    192.168.1.143:50761    104.18.27.48:443       ESTABLISHED     14908
  TCP    192.168.1.143:50763    31.13.87.1:443         ESTABLISHED     14908
  TCP    192.168.1.143:50765    43.174.225.10:443      ESTABLISHED     14908
  TCP    192.168.1.143:50769    31.13.87.1:443         ESTABLISHED     14908
  TCP    192.168.1.143:50776    140.82.114.25:443      ESTABLISHED     14908
  TCP    192.168.1.143:50807    146.75.46.137:443      ESTABLISHED     14908
  TCP    192.168.1.143:50817    52.17.119.191:8282     ESTABLISHED     14908
  TCP    192.168.1.143:50825    34.36.213.229:443      ESTABLISHED     14908
  TCP    192.168.1.143:50827    34.36.213.229:443      ESTABLISHED     14908
  TCP    192.168.1.143:50828    3.169.36.96:443        ESTABLISHED     14908
  TCP    192.168.1.143:50838    146.75.93.91:443       ESTABLISHED     14908
  TCP    192.168.1.143:50841    146.75.93.91:443       ESTABLISHED     14908
```

- I found a connection that connect to `8282` port. It's not usaul to see. So I assume it to be abnormal.

```
TCP    192.168.1.143:50807    146.75.46.137:443      ESTABLISHED     14908
TCP    192.168.1.143:50817    52.17.119.191:8282     ESTABLISHED     14908
TCP    192.168.1.143:50825    34.36.213.229:443      ESTABLISHED     14908
```

Then I try to investigate the IP address and port.

- `whois 52.17.119.191`

It shows that this IP address is host at a AWS machine. And It locate at I

```
└─$ whois 52.17.119.191

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#



# start

NetRange:       52.0.0.0 - 52.79.255.255
CIDR:           52.64.0.0/12, 52.0.0.0/10
NetName:        AT-88-Z
NetHandle:      NET-52-0-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        1991-12-19
Updated:        2024-02-05
Comment:        Geofeed http://ip-ranges.amazonaws.com/geo-ip-feed.csv
Ref:            https://rdap.arin.net/registry/ip/52.0.0.0



OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
```

- nslookup reverse lookup (IP to Domain name): `nslookup 52.17.119.191` .

```
└─$ nslookup 52.17.119.191
191.119.17.52.in-addr.arpa      name = ec2-52-17-119-191.eu-west-1.compute.amazonaws.com.

Authoritative answers can be found from:
```

> Looks like a AWS server

- Use nmap to check the service name at `8282` port

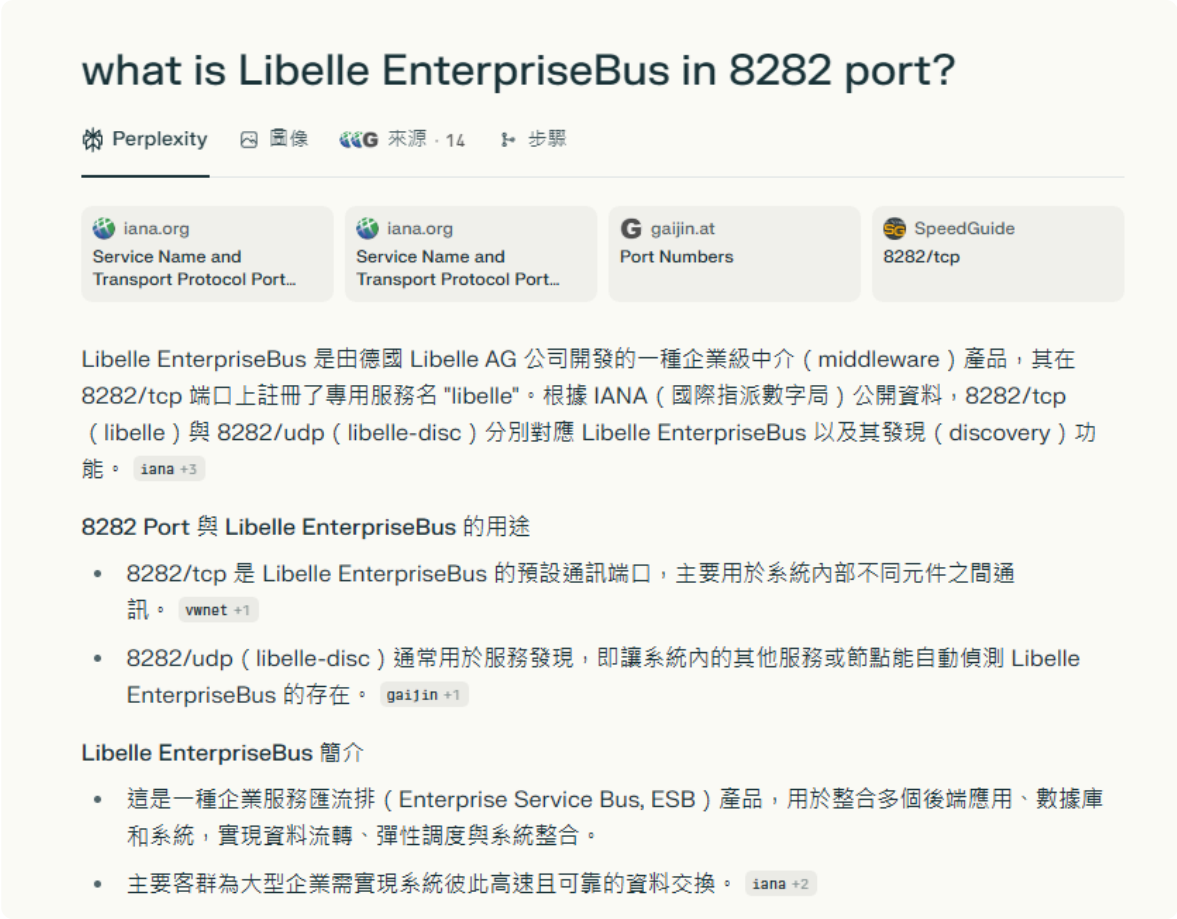
```
└─$ nmap -sV -sC 52.17.119.191 -p 8282
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 09:30 CST
Nmap scan report for ec2-52-17-119-191.eu-west-1.compute.amazonaws.com (52.17.119.191)
Host is up (0.0010s latency).

PORT     STATE    SERVICE VERSION
8282/tcp filtered libelle

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

- Check the service name: `libelle`

8282	libelle	TCP	Libelle EnterpriseBus	Registered: 2016-02-17
8282	libelle-disc	UDP	Libelle EnterpriseBus discovery	Registered: 2016-02-17
8282		SCTP/DCCP	Reserved	

ref: https://www.gaijin.at/en/infos/port-numbers?page=13
(https://www.gaijin.at/en/infos/port-numbers?page=13)

- Gain more information in `libelle`



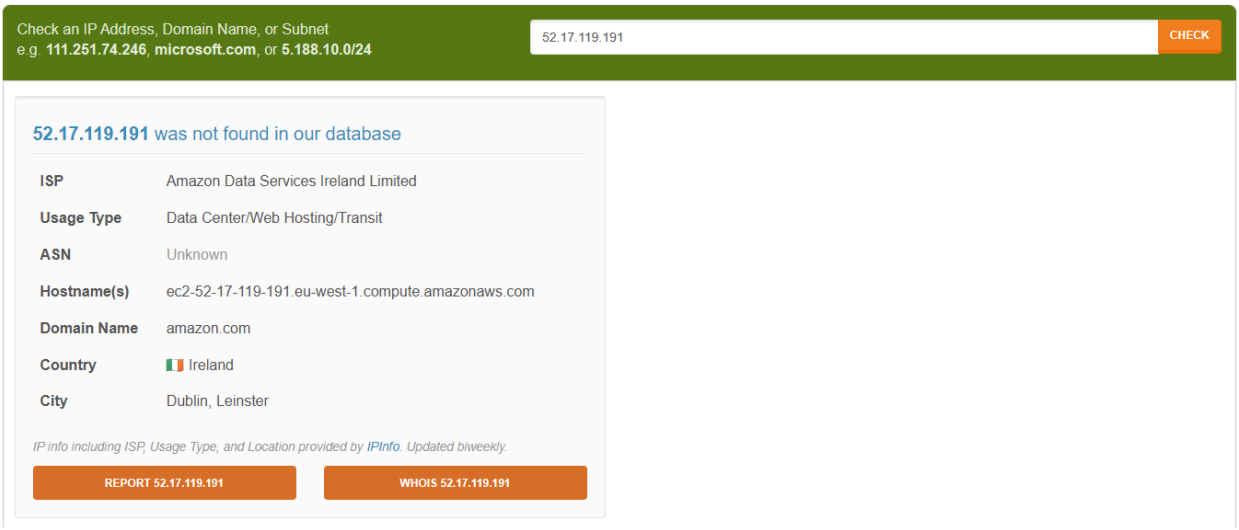
ref: perplexity

- Check the process: `tasklist /FI "PID eq 14908"` .
  Shows that PID is from my browser executable file. So I consider that could be normal.

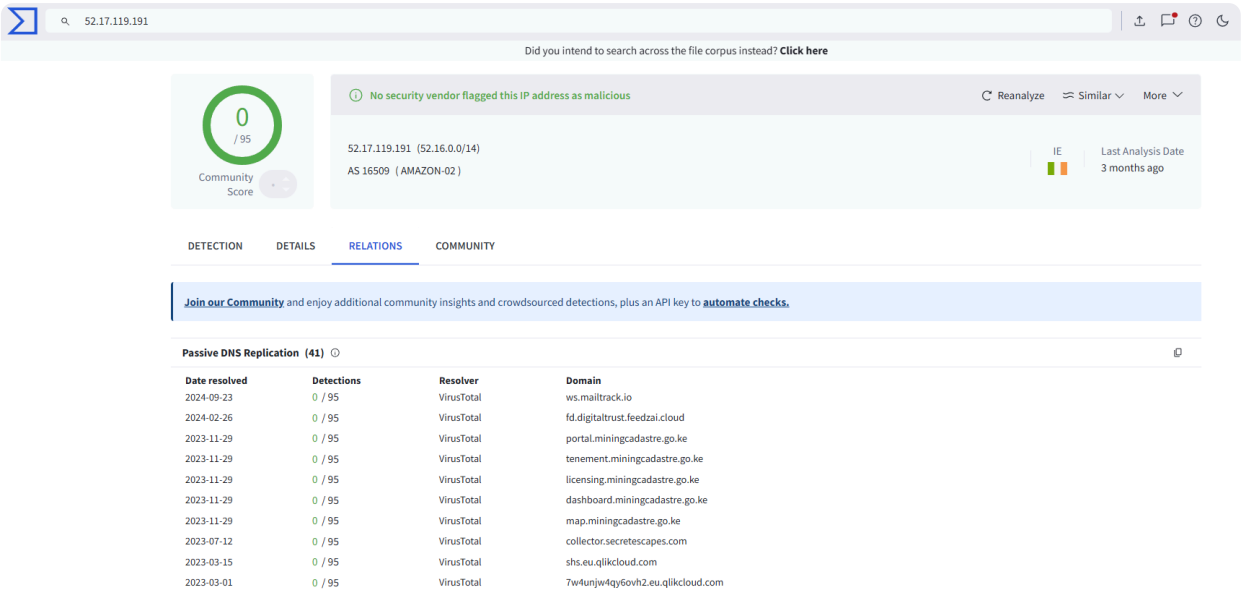
```
  TCP    192.168.1.143:50807    146.75.46.137:443      ESTABLISHED     14908
  TCP    192.168.1.143:50817    52.17.119.191:8282     ESTABLISHED     14908
  TCP    192.168.1.143:50825    34.36.213.229:443      ESTABLISHED     14908
C:\Users\foren>tasklist /FI "PID eq 14908"

映像名稱                       PID 工作階段名稱        工作階段 #    RAM使用量
========================= ======== ================ =========== ============
brave.exe                    14908 Console                    7     72,068 K
```

- Use AbuseIPDB check it seems no abnormal.

AbuseIPDB » *52.17.119.191*



- Using virustoal check it seems to be safe.



- Check which extension use it.

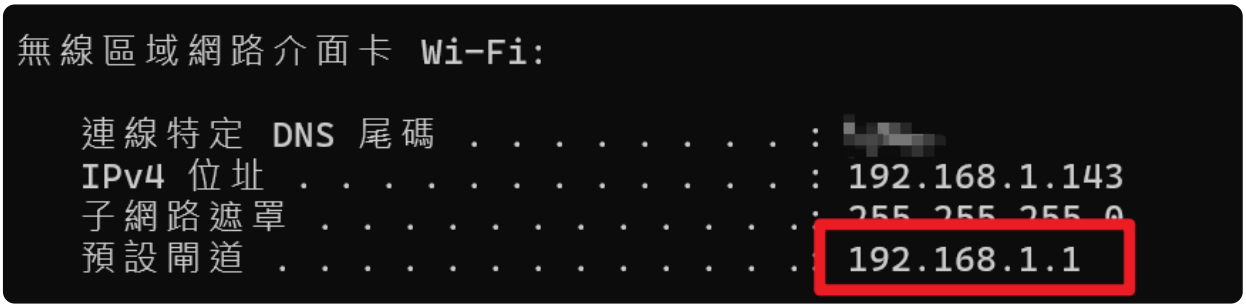
  I search the IP address `52.17.119.191` in google. And finally know that this IP is come from "Mailsuite" extension.

- 54.194.36.47
- 34.246.13.131
- 54.171.22.33
- 54.77.56.1
- 52.17.119.191
- 52.18.207.76
- 52.209.92.165
- 54.170.30.185
- 52.17.119.201
- 52.48.72.84

> ref: https://mailsuite.com/hc/en-us/articles/17628486344477-Whitelist-Mailsuite-IPs (https://mailsuite.com/hc/en-us/articles/17628486344477-Whitelist-Mailsuite-IPs)

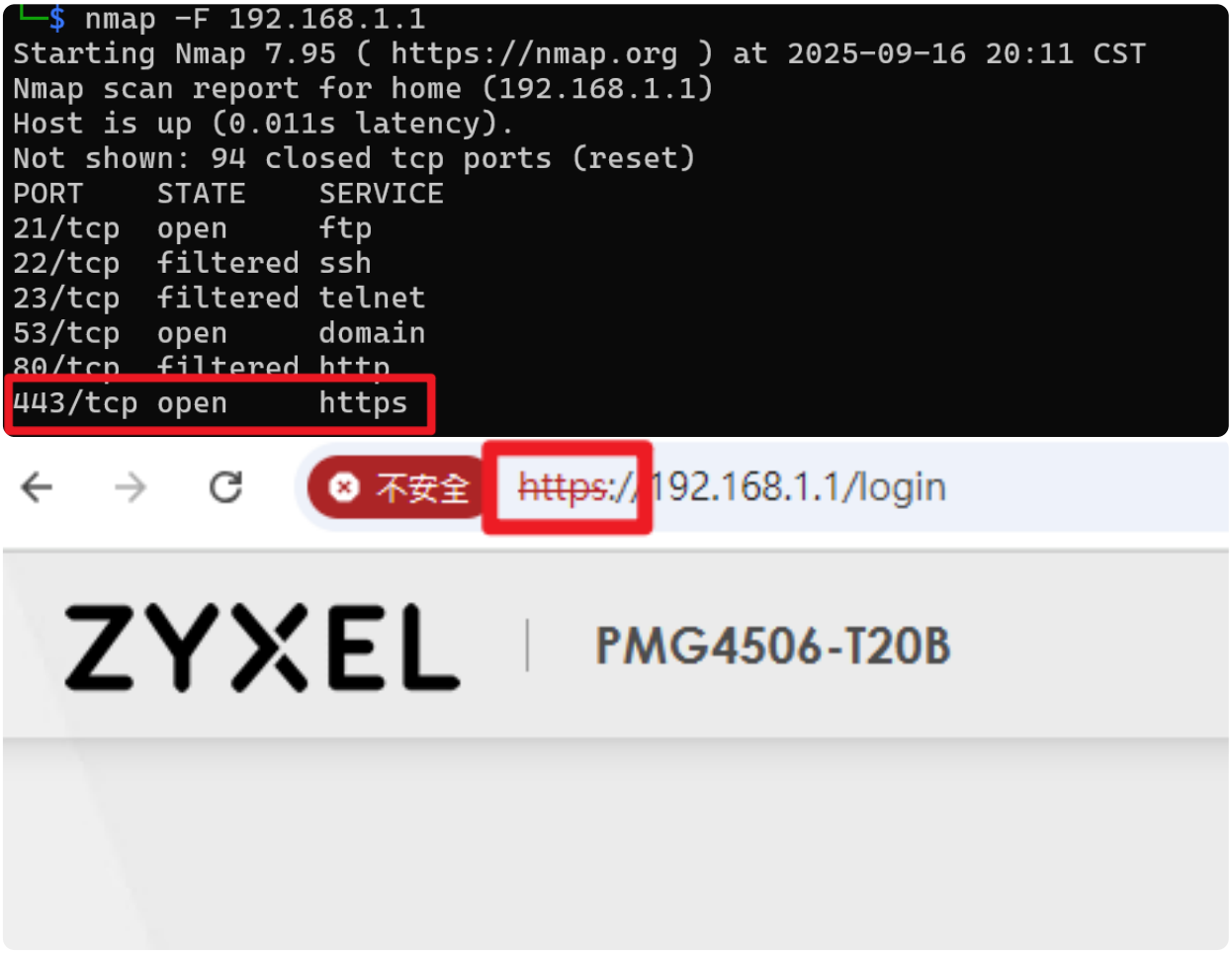
Investigating the Network Environment

- `ipconfig` to check my gateway.



- Access to gateway. And shows that I can't connect to it.

- `nmap -F 192.168.1.1` . found that I need to use `443` port to access



- But the management dashboard has not Log file. So I'm not going to deep dive into it.

Reflection

In this report. I try to use the command line interface to check different network information to find the abnormal process and flow. When I see some connectio or information are different with each others. I will assume it could be malicious or abnormal. Then try to investigate the information and deep dive into it. Later, I can get the whole picture by the incident. And distinguish perhaps it is malicious or not.