ViewSonic
vCast Security Testing Report (vCast 資安測試報告)

The test is conducted on 16th November,2023 with the environment setting up on the testing machine on following specification on network capture:

Testing Devices:
Android: ViewSonic Interactive IFP: IFP8652
Windows: Windows 10 22H2 on VM

The specification of the network capture machine (網路封包測試機器)

Wireshark version:	4.0.10 (v4.0.10-0-gf5c7c25a81eb)
Python3 version:	3.11.6
OS version:	macOS 13.5.2
Memory:	16 GB
CPU:	Apple M2

To ensure integrity and security of the self-developed tool, the tool had been scanned with following reports:

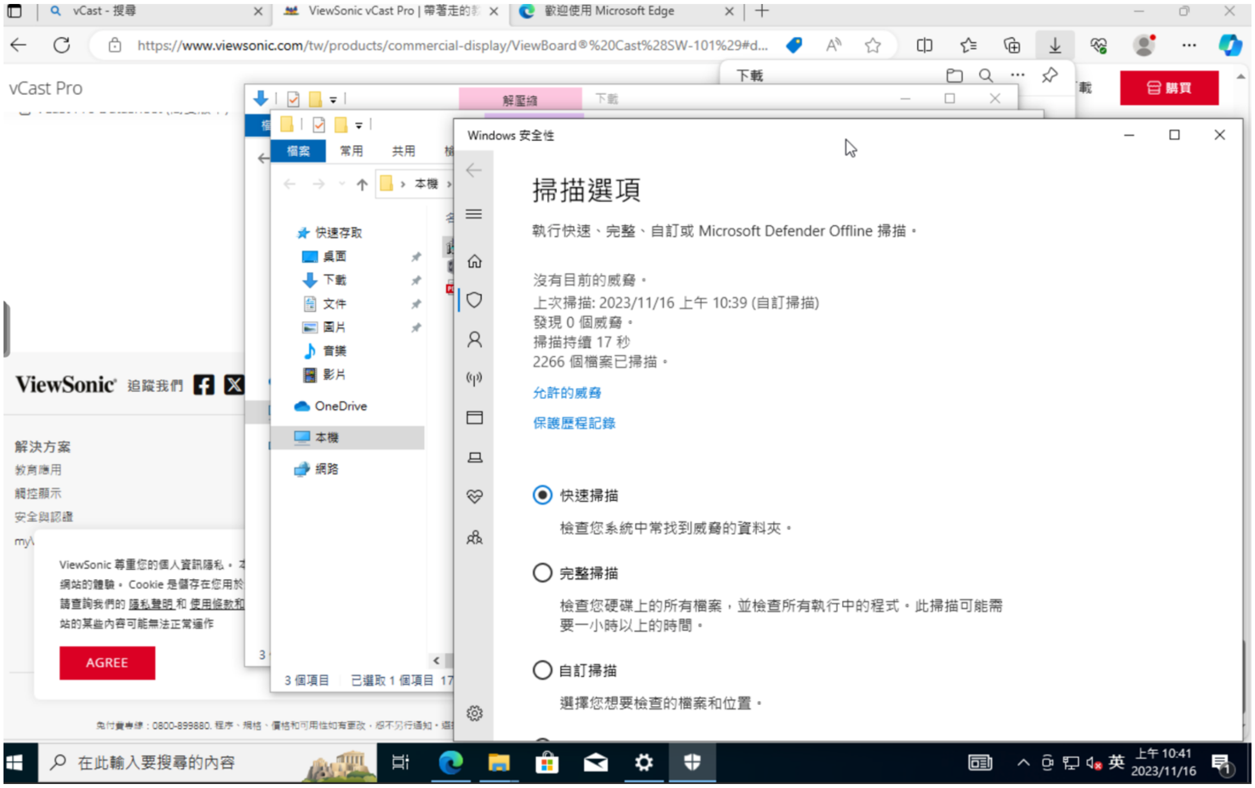
Tools:
The ViewSonic self-developed tool used to figure out the distinct record on IP and their location through (ipinfo) in the PCAP file
https://tinyurl.com/yve3vzez

Source-code scanning report:
https://tinyurl.com/yorpe78o

.................Column Break.................The testing mainly for scoping vCast software on ViewSonic IFP had security assessments on Windows-Based Agent, Android Receiver and Network captures. Such testing had been successfully done on 16th November 2023 10:00-13:10(Taipei Time) and the result as follows:

(此資安檢測的範圍為 ViewSonic IFP 上面的 vCast 軟體包含 Windows 版本，安卓版本，以及傳送的網路封包的資訊安全。此測試執行日期為台北時間 2023 年十一月十六日上午十點至下午一點十分，並經由 Bureau Veritas 公司專業資安專家在旁檢視並確認檢測結果。)

1) Windows Agent (vCastPro - Windows 版本)
   vCastPro version: 3.5.851
   Result: As expected, and passed the Windows Defender with no vulnerability as screen capped below(測試結果通過，經微軟資安工具掃描結果沒有漏洞):



ViewSonic 尊重您的個人資訊隱私。本
網站的體驗。Cookie 是儲存在您用於
請查詢我們的 隱私聲明 和 使用條款和
站的某些內容可能無法正常運作

免付費專線：0800-899880. 程序、規格、價格和可用性如有更改，恕不另行通知。

Windows 安全性

掃描選項

執行快速、完整、自訂或 Microsoft Defender Offline 掃描。

沒有目前的威脅。
上次掃描: 2023/11/16 上午 10:39 (自訂掃描)
發現 0 個威脅。
掃描持續 17 秒
2266 個檔案已掃描。

允許的威脅

保護歷程記錄

● 快速掃描

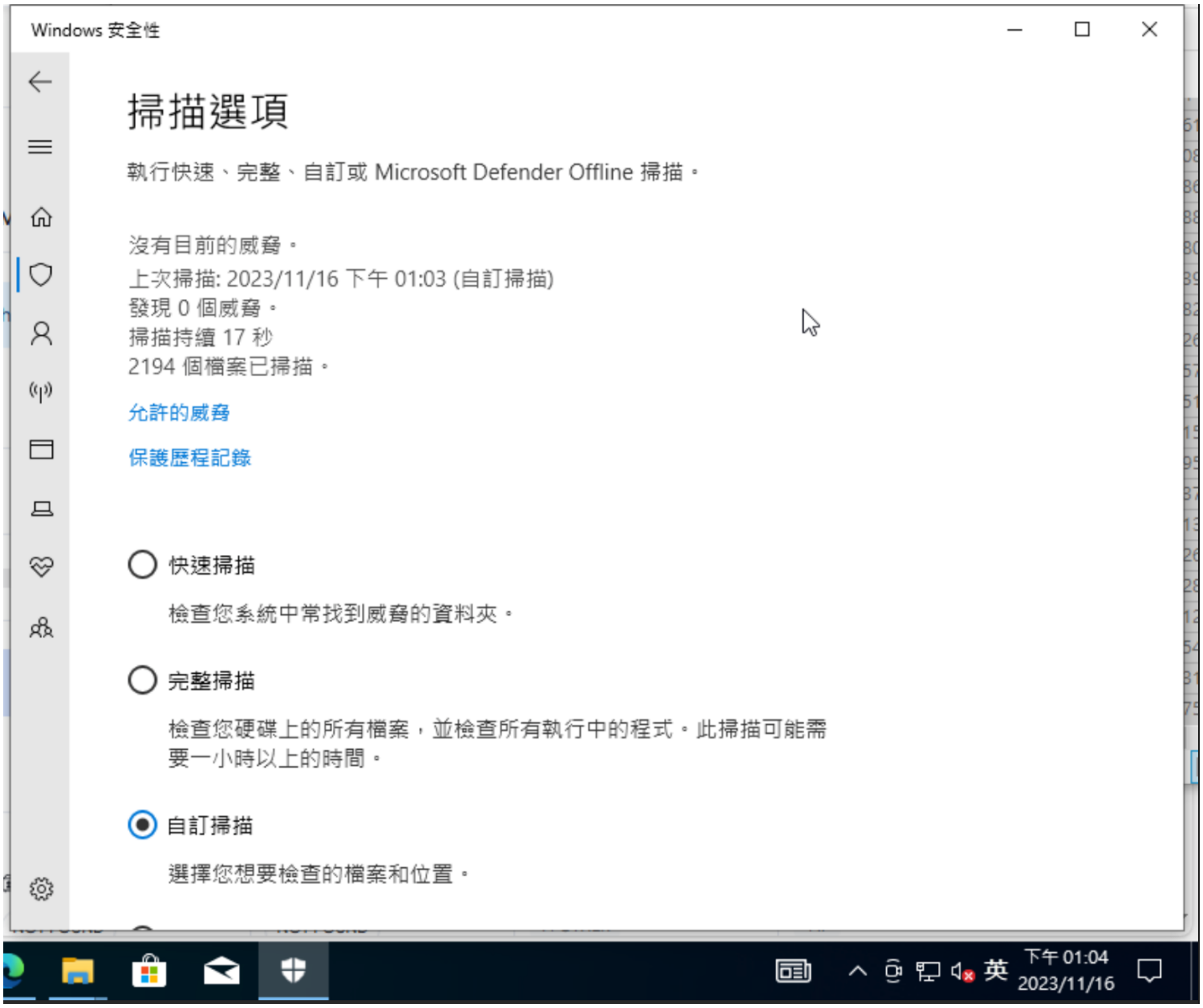
檢查您系統中常找到威脅的資料夾。

○ 完整掃描

檢查您硬碟上的所有檔案，並檢查所有執行中的程式。此掃描可能需要一小時以上的時間。

○ 自訂掃描

選擇您想要檢查的檔案和位置。



掃描選項

執行快速、完整、自訂或 Microsoft Defender Offline 掃描。

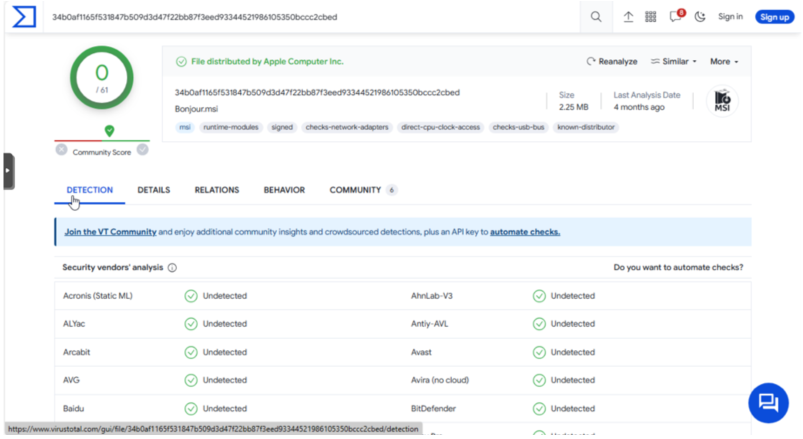
沒有目前的威脅。
上次掃描: 2023/11/16 下午 01:03 (自訂掃描)
發現 0 個威脅。
掃描持續 17 秒
2194 個檔案已掃描。

○ 快速掃描
檢查您系統中常找到威脅的資料夾。

○ 完整掃描
檢查您硬碟上的所有檔案，並檢查所有執行中的程式。此掃描可能需要一小時以上的時間。

● 自訂掃描
選擇您想要檢查的檔案和位置。

In the testing besides vCast.exe, we also found there are 3 other exe/msi file that on the directory. The Bonjour.msi/Bonjour64.msi/AutoHomeServer.exe was marked clean in VirusTotal.
(此測試包含除 vCast.exe 之外的目錄內另外 3 個執行檔，經專業資安工具 Virustotal 檢驗後均無資安風險疑慮)：



34b0af1165f531847b509d3d47f22bb87f3eed93344521986105350bccc2cbed

File distributed by Apple Computer Inc.

34b0af1165f531847b509d3d47f22bb87f3eed93344521986105350bccc2cbed
Bonjour.msi

Size: 2.25 MB
Last Analysis Date: 4 months ago

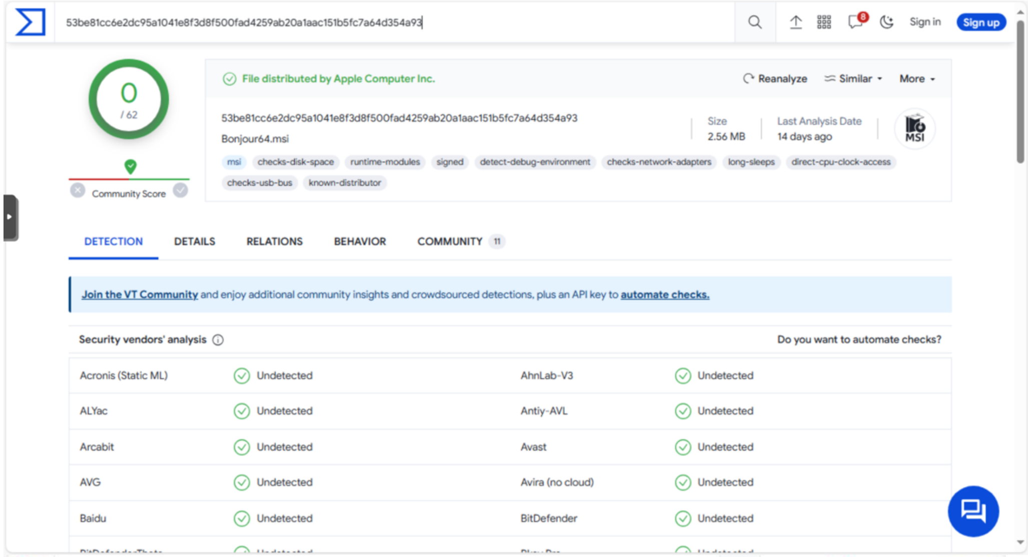
msi · runtime-modules · signed · checks-network-adapters · direct-cpu-clock-access · checks-usb-bus · known-distributor

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected

https://www.virustotal.com/gui/file/34b0af1165f531847b509d3d47f22bb87f3eed93344521986105350bccc2cbed/detection



53be81cc6e2dc95a1041e8f3d8f500fad4259ab20a1aac151b5fc7a64d354a93

0 / 62

File distributed by Apple Computer Inc.

53be81cc6e2dc95a1041e8f3d8f500fad4259ab20a1aac151b5fc7a64d354a93
Bonjour64.msi

Size 2.56 MB

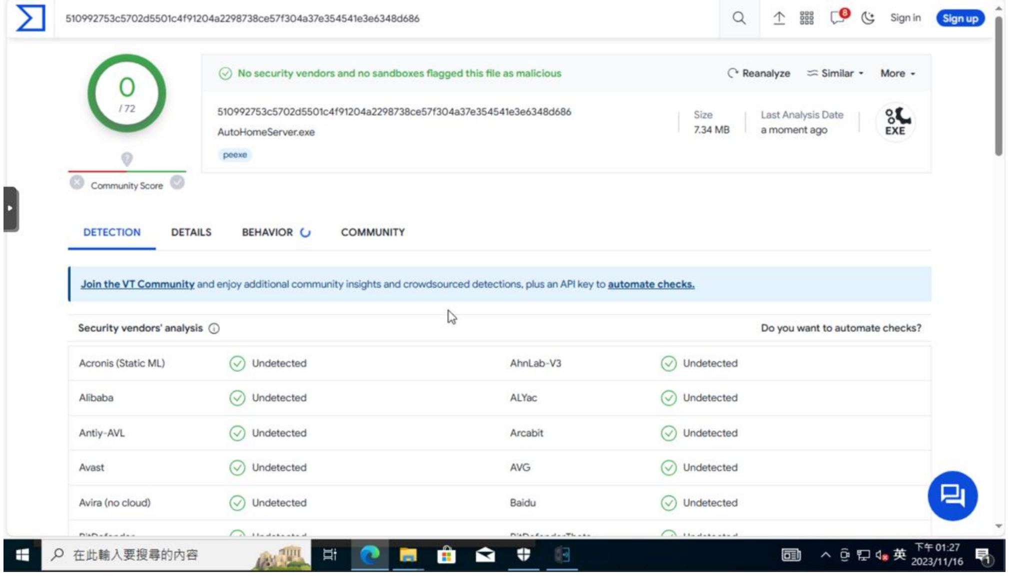
Last Analysis Date 14 days ago

msi checks-disk-space runtime-modules signed detect-debug-environment checks-network-adapters long-sleeps direct-cpu-clock-access checks-usb-bus known-distributor

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ — Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected



510992753c5702d5501c4f91204a2298738ce57f304a37e354541e3e6348d686

0 / 72

No security vendors and no sandboxes flagged this file as malicious

510992753c5702d5501c4f91204a2298738ce57f304a37e354541e3e6348d686
AutoHomeServer.exe

Size 7.34 MB

Last Analysis Date a moment ago

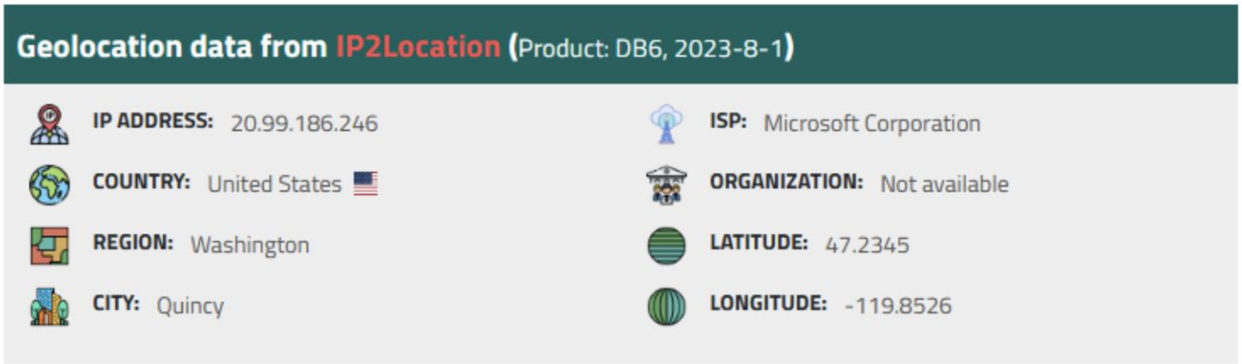
peexe

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ — Do you want to automate checks?

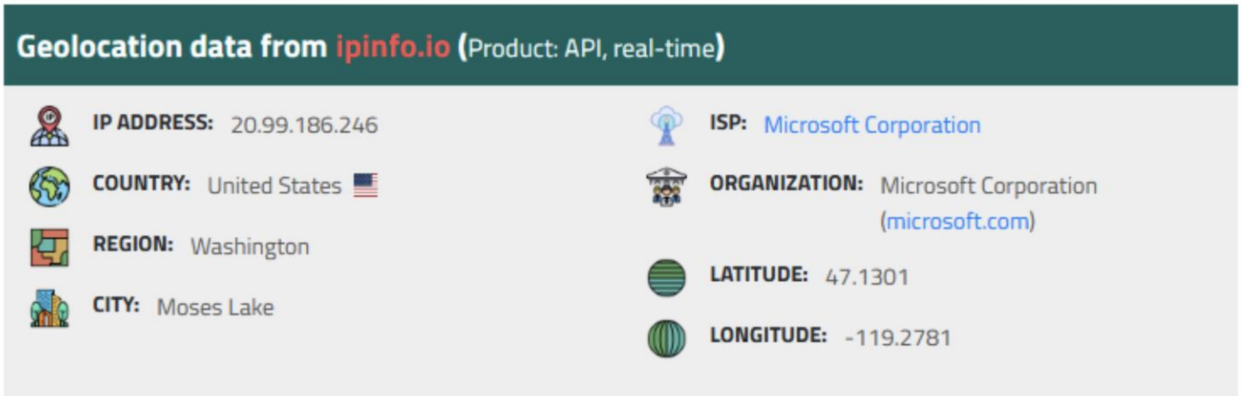
Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected

Second, the IP address linking in the report are checked and only connect to CDN networks:(執行檔的 IP 連結均為美國，非連結至中國)



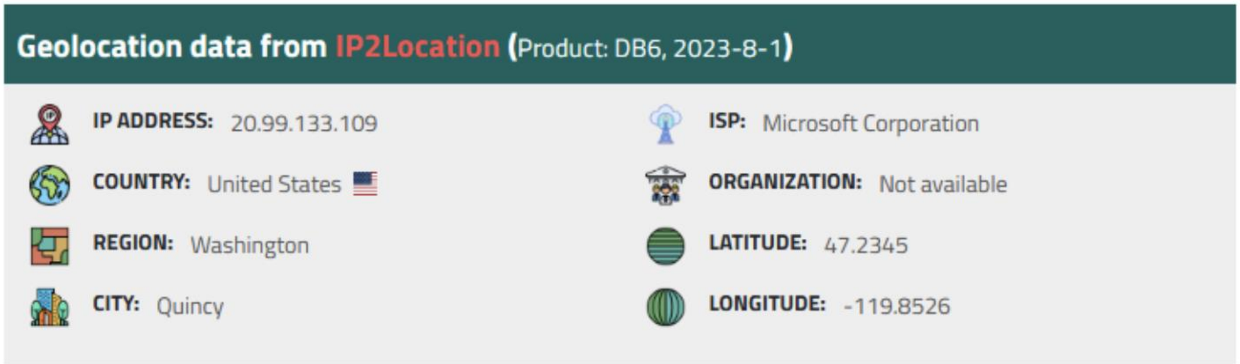
Geolocation data from IP2Location (Product: DB6, 2023-8-1)

IP ADDRESS:	20.99.186.246	ISP:	Microsoft Corporation
COUNTRY:	United States	ORGANIZATION:	Not available
REGION:	Washington	LATITUDE:	47.2345
CITY:	Quincy	LONGITUDE:	-119.8526



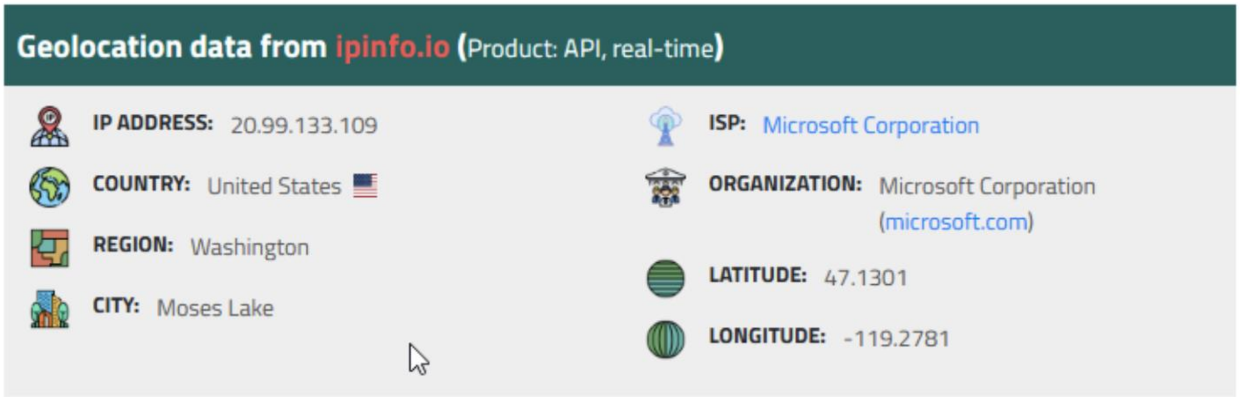
Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS:	20.99.186.246	ISP:	Microsoft Corporation
COUNTRY:	United States	ORGANIZATION:	Microsoft Corporation (microsoft.com)
REGION:	Washington	LATITUDE:	47.1301
CITY:	Moses Lake	LONGITUDE:	-119.2781



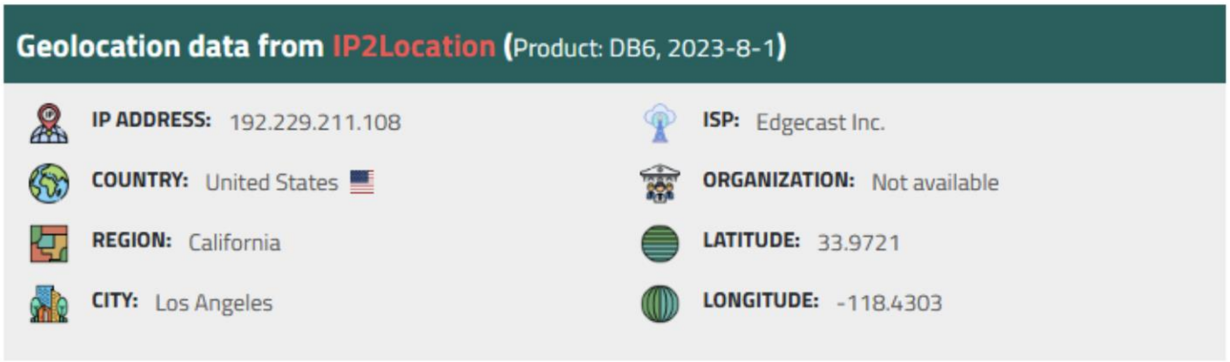
Geolocation data from IP2Location (Product: DB6, 2023-8-1)

IP ADDRESS:	20.99.133.109	ISP:	Microsoft Corporation
COUNTRY:	United States	ORGANIZATION:	Not available
REGION:	Washington	LATITUDE:	47.2345
CITY:	Quincy	LONGITUDE:	-119.8526



Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS:	20.99.133.109	ISP:	Microsoft Corporation
COUNTRY:	United States	ORGANIZATION:	Microsoft Corporation (microsoft.com)
REGION:	Washington	LATITUDE:	47.1301
CITY:	Moses Lake	LONGITUDE:	-119.2781



Geolocation data from IP2Location (Product: DB6, 2023-8-1)

IP ADDRESS: 192.229.211.108

COUNTRY: United States 🇺🇸

REGION: California

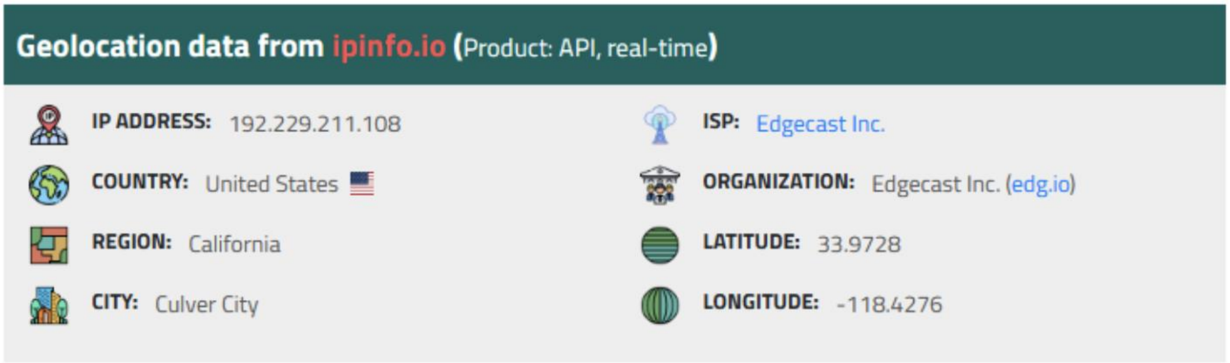
CITY: Los Angeles

ISP: Edgecast Inc.

ORGANIZATION: Not available

LATITUDE: 33.9721

LONGITUDE: -118.4303



Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 192.229.211.108

COUNTRY: United States 🇺🇸

REGION: California

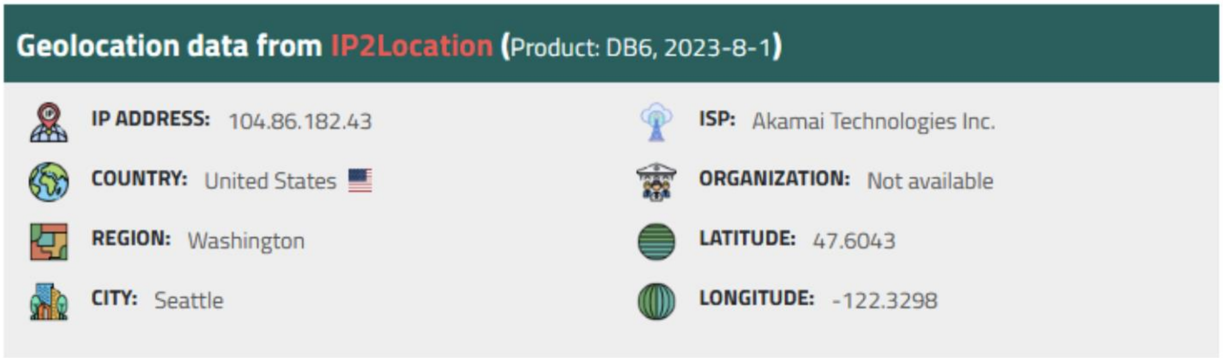
CITY: Culver City

ISP: Edgecast Inc.

ORGANIZATION: Edgecast Inc. (edg.io)

LATITUDE: 33.9728

LONGITUDE: -118.4276



Geolocation data from IP2Location (Product: DB6, 2023-8-1)

IP ADDRESS: 104.86.182.43

COUNTRY: United States 🇺🇸

REGION: Washington

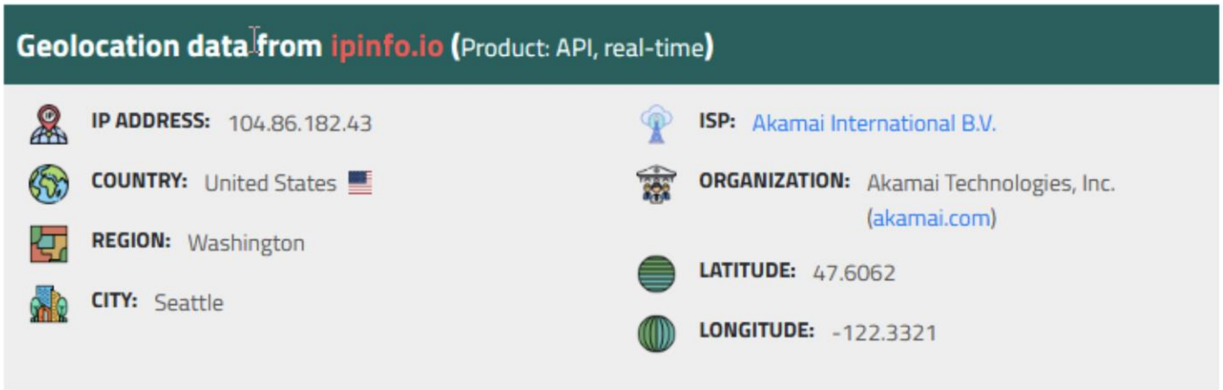
CITY: Seattle

ISP: Akamai Technologies Inc.

ORGANIZATION: Not available

LATITUDE: 47.6043

LONGITUDE: -122.3298



Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 104.86.182.43

COUNTRY: United States 🇺🇸

REGION: Washington

CITY: Seattle

ISP: Akamai International B.V.

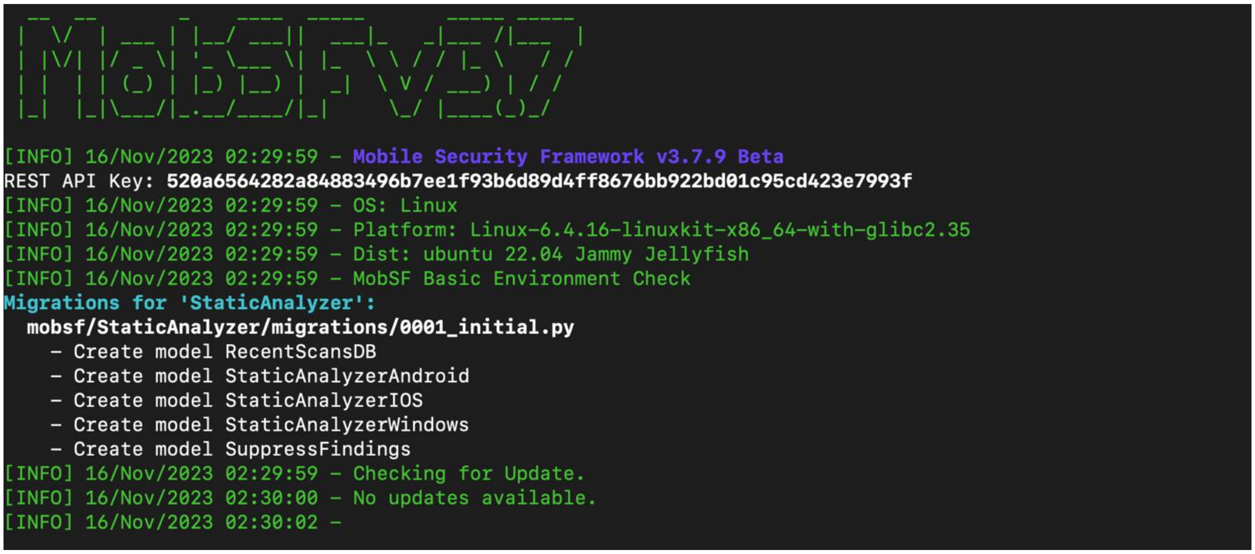
ORGANIZATION: Akamai Technologies, Inc. (akamai.com)

LATITUDE: 47.6062

LONGITUDE: -122.3321

..................Column Break..................2) Android APK with following info (vCast 安卓版本)

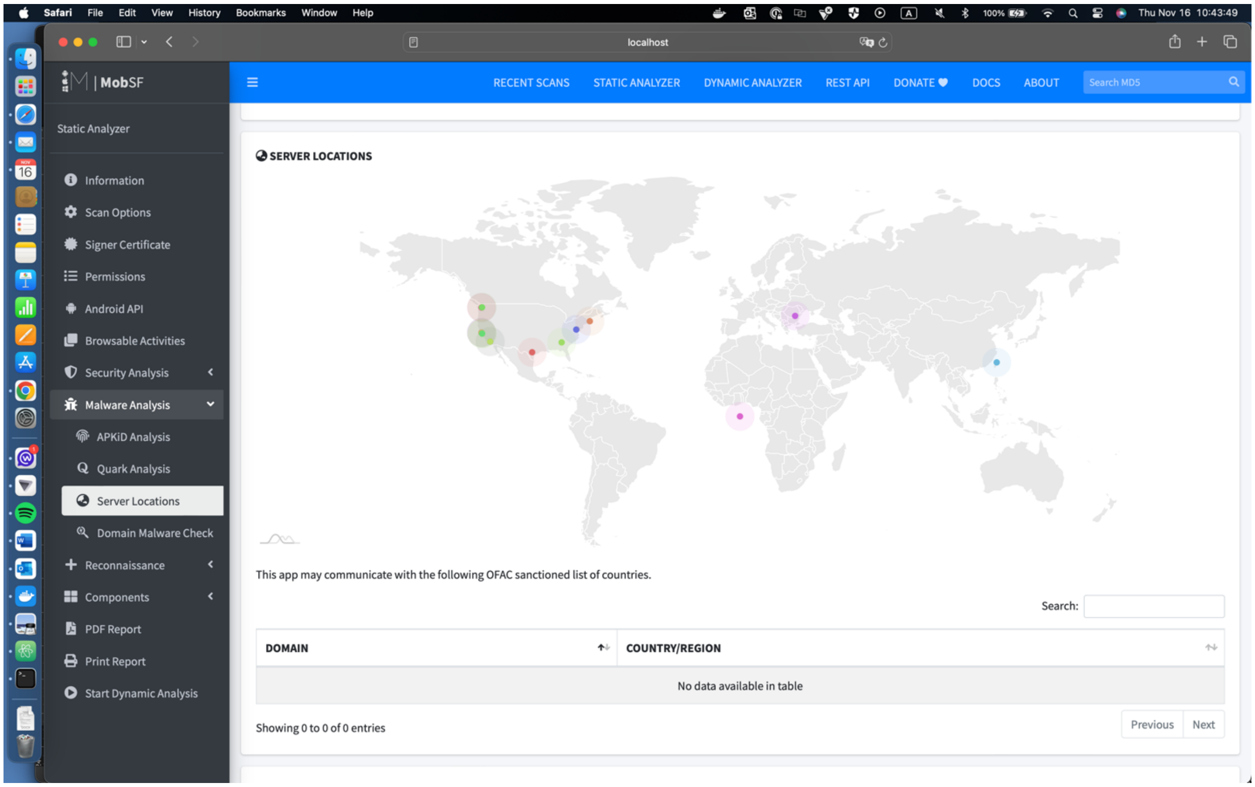
vCastReceiver_v2.4.1114_4 in 1-2.apk.1_signed.apk
MD5 = db97a0c1040c8301b5fa3e6617b3d467
SHA256 = ba501cfe2e4ded9d31b4d6c22668fc309698dcb653f5e86e4e1164f071be52af
The MobSF version used as below:



```
  __  __       _    ____  _____       _____ _____
 |  \/  | ___ | |__/ ___||  ___|_   _|___ /|___  |
 | |\/| |/ _ \| '_ \___ \| |_  \ \ / / |_ \   / /
 | |  | | (_) | |_) |__) |  _|  \ V / ___) | / /
 |_|  |_|\___/|_.__/____/|_|     \_/ |____(_)_/

[INFO] 16/Nov/2023 02:29:59 - Mobile Security Framework v3.7.9 Beta
REST API Key: 520a6564282a84883496b7ee1f93b6d89d4ff8676bb922bd01c95cd423e7993f
[INFO] 16/Nov/2023 02:29:59 - OS: Linux
[INFO] 16/Nov/2023 02:29:59 - Platform: Linux-6.4.16-linuxkit-x86_64-with-glibc2.35
[INFO] 16/Nov/2023 02:29:59 - Dist: ubuntu 22.04 Jammy Jellyfish
[INFO] 16/Nov/2023 02:29:59 - MobSF Basic Environment Check
Migrations for 'StaticAnalyzer':
  mobsf/StaticAnalyzer/migrations/0001_initial.py
    - Create model RecentScansDB
    - Create model StaticAnalyzerAndroid
    - Create model StaticAnalyzerIOS
    - Create model StaticAnalyzerWindows
    - Create model SuppressFindings
[INFO] 16/Nov/2023 02:29:59 - Checking for Update.
[INFO] 16/Nov/2023 02:30:00 - No updates available.
[INFO] 16/Nov/2023 02:30:02 -
```

Result: As expected, and passed the test as the screen cap below (通過，透過 APP 資安掃描工具 MobSF 掃描結果並無資安漏洞):



SERVER LOCATIONS

This app may communicate with the following OFAC sanctioned list of countries.

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

3) Network capture file with hash

Pcap1: 20231116-1038.pcapng
MD5: b254b18182d16acb97e520461eba6acd
Pcap2: 20231116-1109.pcapng
MD5: 086bcfe3325453254eaa7f9dbc705a84

Pcap3: 20231116-1140.pcapng

MD5: b4131643c8e9c922dbd1033ccf61fec5

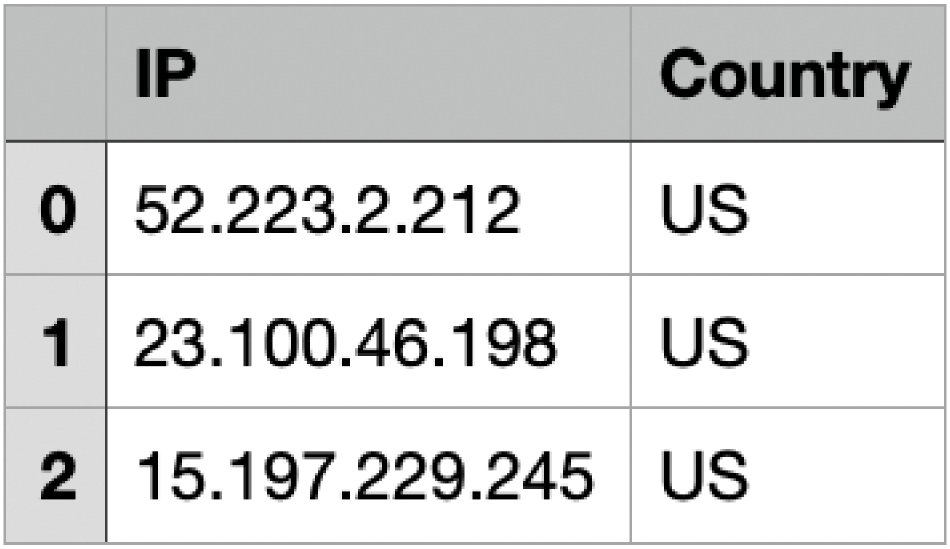
Pcap4: 20231116-1210.pcapng
MD5: 3eefa8c4b635f438303bb1c161f2b0a1

Result: all PCAP file captured the transaction and test result as expected in the plan
The distinct list of IP in such list as below(測試結果：所有網路封包測錄結果正常，IP 結果如下，均無中國 IP):

20231116-1038

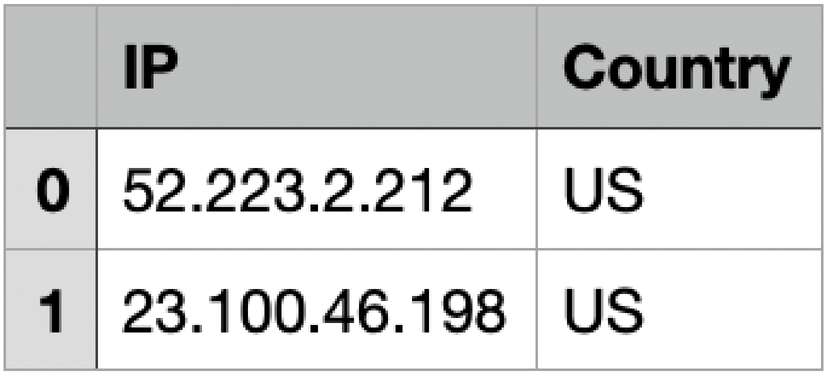
	IP	Country
0	52.218.220.56	US
1	3.33.230.82	US
2	75.2.66.225	US
3	52.177.138.113	US
4	20.212.88.141	SG
5	15.197.229.245	US
6	35.71.150.102	US
7	52.218.237.152	US
8	52.223.2.212	US
9	52.29.145.193	DE
10	172.217.160.99	TW
11	142.251.42.234	TW
12	142.251.42.227	TW
13	172.217.163.46	TW
14	142.251.43.14	TW
15	23.92.19.217	US
16	97.64.45.39	US
17	23.100.46.198	US

20231116-1109



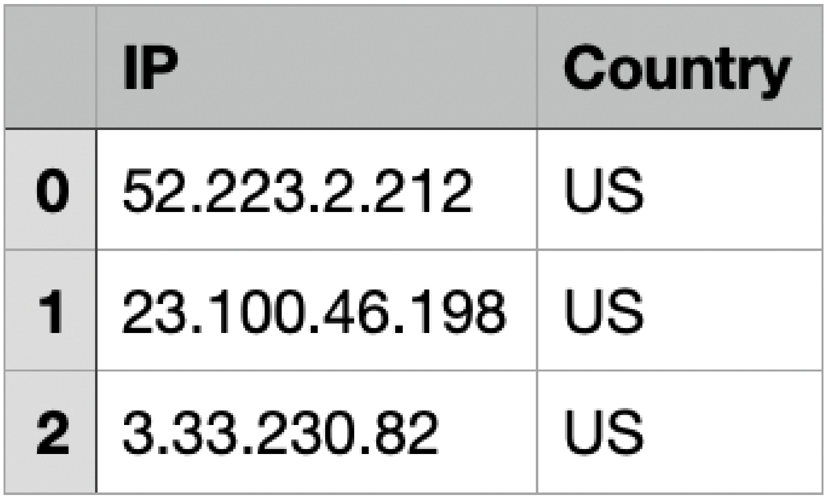
	IP	Country
0	52.223.2.212	US
1	23.100.46.198	US
2	15.197.229.245	US

20231116-1140



	IP	Country
0	52.223.2.212	US
1	23.100.46.198	US

20231116-1210



	IP	Country
0	52.223.2.212	US
1	23.100.46.198	US
2	3.33.230.82	US