TPI

Reported

MuMuPlayer

Emulator

Analysis

Contact:

Hao Ding

Date:

Sep 4, 2025 2:02 AM

Objective

Based

on

one

TPI-

reported

confirmed

emulator

usage

case,

we

extended

the

scope

to

all

login

events

with

similar

characteristics,

observed

per

this

case’s

review,

for

the

month

of

July

2025

and

conducted

data

profiling(user

active

rate,

physical

card

activation

rate,

DDer

rate

etc.)

Initial

Discovery

Summary

-

Case

Identified

:

User

86963958

confirmed

using

MuMuPlayer

emulator

per

TPI’s

report

-

Key

Signal

:

Login

request

info

shows

some

mismatch:

1.

Network

Carrier

:

FarEasTone

(Taiwan-based

telecom)

2.

IP

Carrier

Info

:

U.S.

location,

provider

=

Charter

Communications

Inc.

-

Finding

&

Hypothesis

:

●

This

case

study

surfaced

that

network

carriers–IP’s

country

mismatch

can

serve

as

a

signal

for

detecting

potential

emulator

usage.

●

However,

potential

false

positives

exist

in

real

user

scenarios,

such

as:

1.

User

in

Taiwan(or

any

foreign

country)

with

local

SIM,

but

accessing

via

VPN

through

a

U.S.

provider

.

2.

User

in

the

U.S.

with

Taiwan/foreign

SIM

card

using

roaming

service

tied

to

a

U.S.

network.

Analysis

Scope

●

Data

Period

:

July

2025

all

successful

logins

●

Focus

:

Accounts

where

network

carrier

country

is

foreign

(non-U.S.)

while

IP

country

is

USA

●

Objective

:

Extend

the

case

study

finding

by

evaluating

whether

network

carrier–IP

country

mismatc

h

is

a

valid

signal

for

emulator

detection

by

observing

differences

in

key

indicators

of

normal

user

behavior

(e.g.,

activity,

card

activation,

payroll

direct

deposit)

within

this

population.

Analysis

Outcome

-

Scale

of

Data

(2025.07

logins)

-

Total

Logins

:

3,123,479

-

Unique

Users

:

1,092,538

-

USA

vs

Foreign

Network

Carrier

Summary(when

IP

Country

is

USA)

(Active

User:

#

of

user

being

in

active

status

as

of

analysis

date

DWN

Logins:

#

of

DWN

session

found

Card

Activated

Users:

#

of

distinct

user

with

physical

card

activated

Payroll

DD

User:

#

of

distinct

users

has

payroll

DDed

with

us)

-

Users

with

foreign

network

carriers

(while

showing

U.S.

IP)

have

significantly

lower

active

user

rates

and

card

activation

rates

compared

to

U.S.

carrier

users.

Their

payroll

direct

deposit

adoption

is

also

markedly

weaker,

further

highlighting

the

engagement

gap.

Metric

USA

Network

Carrier

Foreign

Network

Carrier

Total

Logins

3,100,302

23,177

Total

Users

1,073,862

18,676

Active

Users

1,050,497

6,543

Active

User

%

97.82%

35.03%

DWN

Logins

2,510,072

3,495

DWN

Login

%

80.96%

15.08%

DWN

Users

754,538

1,893

DWN

User

%

70.26%

10.14%

Card

Activated

Users

957,049

2,468

Card

Activated

%

89.12%

13.21%

Payroll

DD

Users

311,292

210

-

Top

Foreign

Network

Carrier

Breakdown((when

IP

Country

is

USA)

-

The

analysis

shows

that

foreign

network

carriers

are

predominantly

from

Taiwan

.

Within

this

group,

user

active

rate

and

other

indicators

of

genuine

engagement

—such

as

card

activation

and

payroll

direct

deposit—

are

much

lower

than

those

of

carriers

from

other

foreign

countries

,

suggesting

a

high

degree

of

signal

consistency

for

detecting

non-genuine

usage.

Conclusion

and

Next

Step

In

July,

logins

from

Taiwan

network

carriers

showed

that

only

about

~33%

of

users

were

still

active,

reflecting

an

unusually

high

inactive

rate.

This

segment

merits

closer

case

review

to

help

us

finalize

detection

logic

with

the

highest

precision

for

synthetic

or

stolen-ID

accounts

.

By

leveraging

ScanID

checks

(login

+

PII

change

time),

we

can

verify

suspicious

accounts

and

enable

batch

action

where

supported.

●

Key

Risk:

Emulator

logins

are

a

high-risk

method,

frequently

tied

to

synthetic/ID

stolen

accounts.

●

Gap

Identified:

Our

current

device

intelligence

failed

to

flag

the

confirmed

emulator

login

in

this

study,

resulting

in

a

false

negative

.

Metric

TWN

IND

NGA

GBR

OTHER\_FOREIGN

Total

Logins

21,602

294

185

135

357

Total

Users

18,053

106

47

101

192

Active

Users

5,965

99

47

45

158

Active

User

%

33.04%

93.40%

100.00%

44.55%

82.29%

DWN

Logins

2,298

250

137

72

289

DWN

Login

%

10.64%

85.03%

74.05%

53.33%

80.95%

DWN

Users

1,378

89

42

48

145

DWN

User

%

7.63%

83.96%

89.36%

47.52%

75.52%

Card

Activated

Users

1,960

92

44

35

127

Card

Activated

%

10.86%

86.79%

93.62%

34.65%

66.15%

Payroll

DD

Users

69

24

8

12

38

Payroll

DD

%

0.38%

22.64%

17.02%

11.88%

19.79%

Going

forward,

strengthening

emulator

detection

and

embedding

it

more

tightly

into

risk

controls

will

be

essential

to

improving

both

coverage

and

accuracy.

Appendix

-

Working

directory

-

Case

study

(confirmed

mumuplayer

case

-

86963958)

-

100

taiwan

network

carrier

202507

logged

in

case