On-Going Research Progress

1

Quick Review

Background

- Mobile Application is a trend right now
- A Lot of applications are published on Google Play
- Meanwhile, Google Play is a “superstar” market (previous research)
- What becomes of the other app?

It Might be Abandoned by its developer (?)

Many Android Apps Use Resource in Internet

Domain Name and IP Address in The Cloud

Research Goal

- Doing a measurement study about app which has been in Google Play for a long time
- Search for abandoned internet resource used by the app
- Hijack the resource and collects data

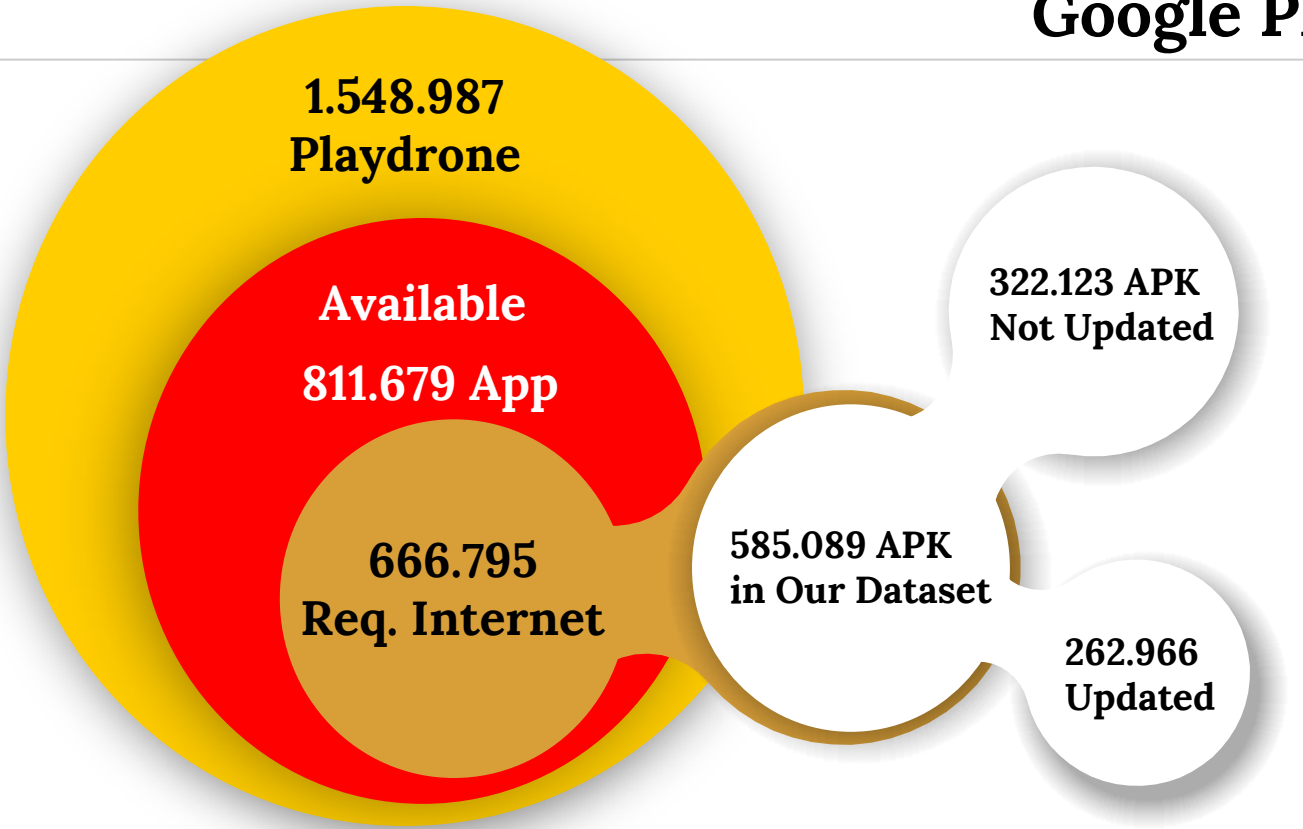
I will be interesting if We find……

- An expired domain which is used in many apps, and these apps were created by same developer
- An expired domain/parked domain which is used by third party library and this library is used by many apps
- Or a developer which has published a lot of apps, but the for some reason stopped their business and leaves a lot of expired domain

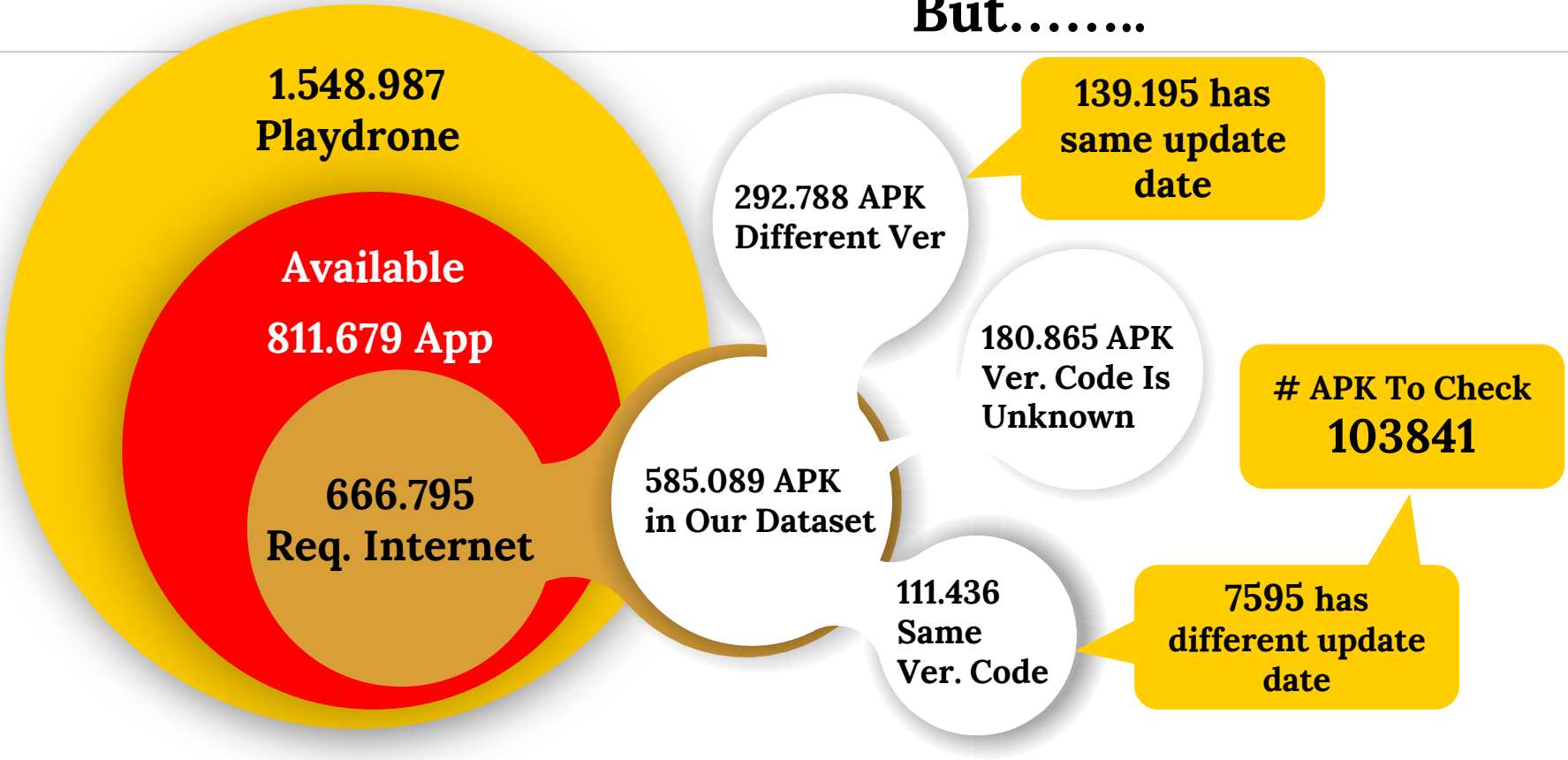
4

Results So Far

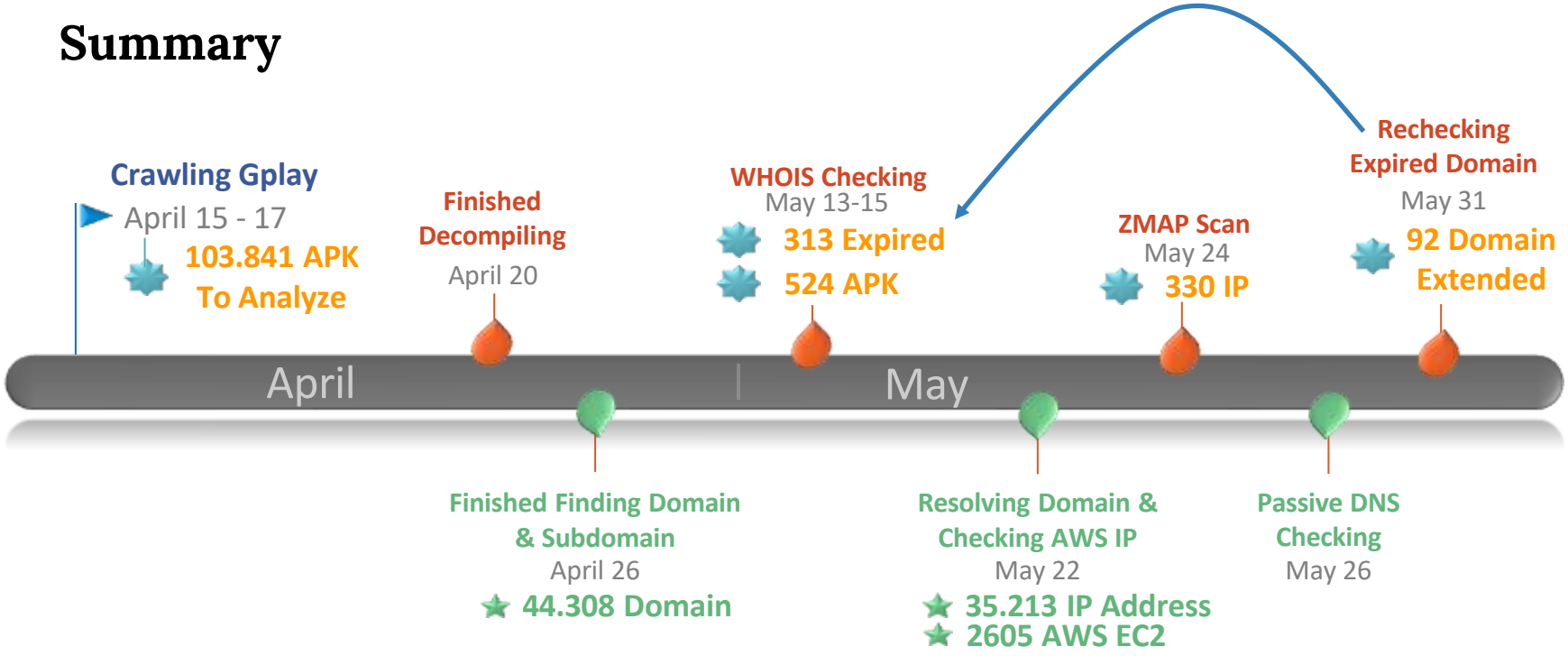
Google Play Availability



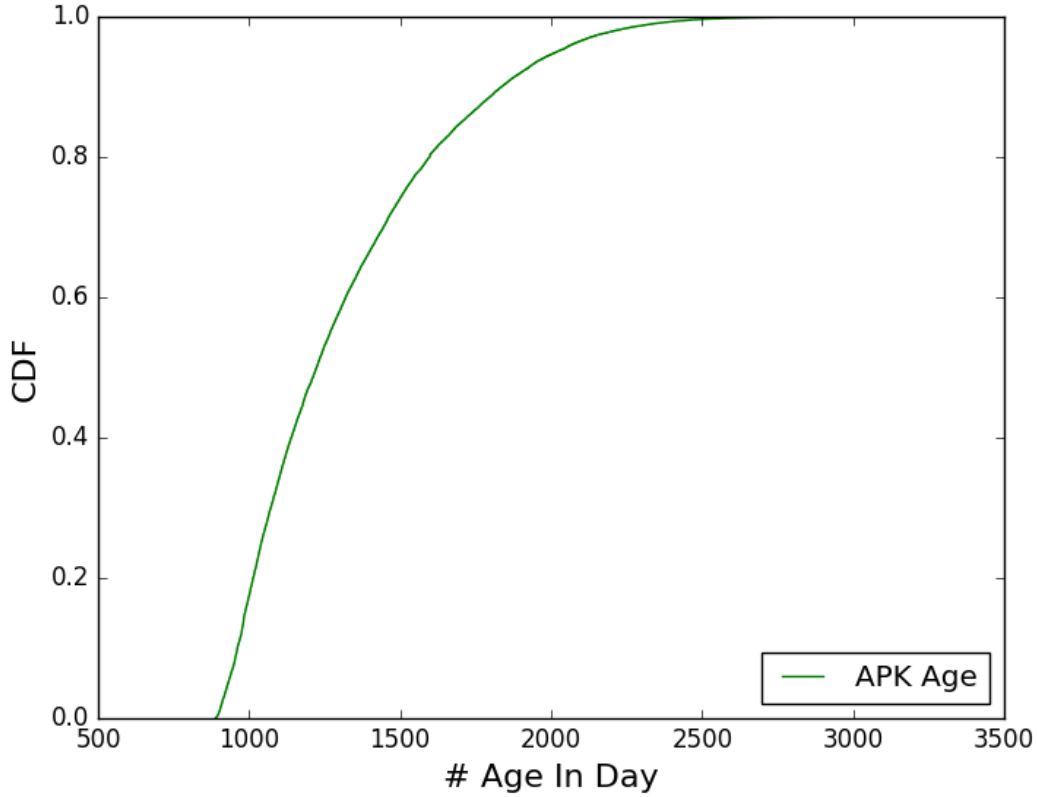
But……


1.548.987
Playdrone
Available
811.679 App
666.795
Req. Internet
585.089 APK
in Our Dataset
292.788 APK
Different Ver
180.865 APK
Ver. Code Is
Unknown
111.436
Same
Ver. Code
139.195 has
same update
date
APK To Check
103841
7595 has
different update
date

Summary


Crawling Gplay
April 15 - 17
103.841 APK
To Analyze
Finished
Decompiling
April 20
WHOIS Checking
May 13-15
313 Expired
524 APK
ZMAP Scan
May 24
330 IP
Rechecking
Expired Domain
May 31
92 Domain
Extended
April
May
Finished Finding Domain
& Subdomain
April 26
44.308 Domain
Resolving Domain &
Checking AWS IP
May 22
35.213 IP Address
2605 AWS EC2
Passive DNS
Checking
May 26

APK Age (103841 APK)



WHOIS Result (1)

Checking Date : 13-15 May 2017

Status	# of Domain
Expired	313 Domain
Not Expired	25.929 Domain
Not Found	1340 Domain
Time Out	35 Domain
Undetermined	16690 Domain
Will Be Expired by the end of May	465 Domain
Will Be Expired In June	1226 Domain

Will Be Checked Again Later

WHOIS Result (2)

- 313 Expired Domain
- 367 Sub domain
- 524 APK

Recheck at 31 May

- 184 Still Expired
- 92 Extend / Reregistered / Domain Parking?
- 35 Undetermined (Open?)
- 2 Time Out

WHOIS Result (3)

At 31 May – rechecked the 16690 Undetermined Domain

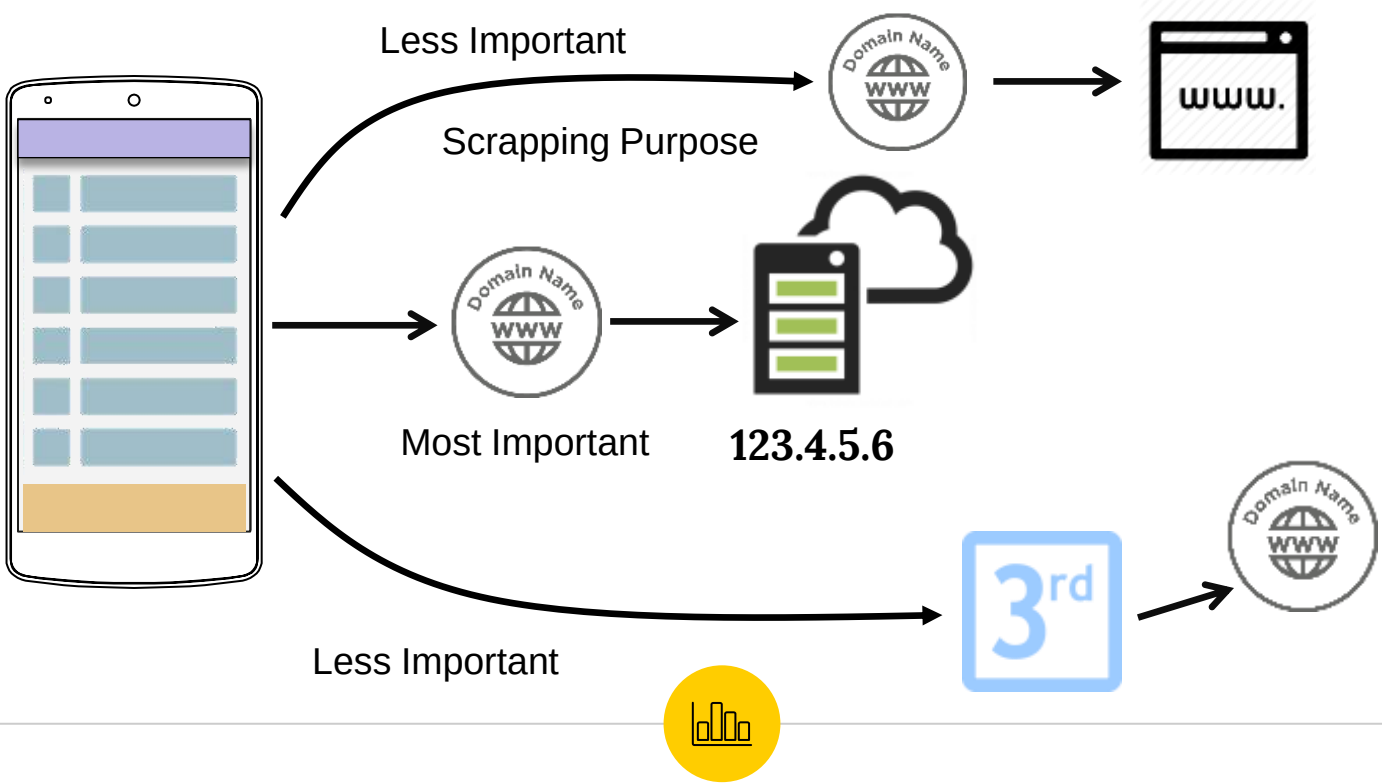
Status	# of Domain
Expired	12 Domain
Not Expired	788 Domain
Time Out	1 Domain
Undetermined	15889 Domain
Will Be Expired In June	23 Domain

WHOIS Result (4)

At 1 June – rechecked the 465 Domain that will be expired in May

Status	# of Domain
Expired	168 Domain
Not Expired	288 Domain
Time Out	1 Domain
Undetermined	7 Domain

The Importance of the Domain for the APP

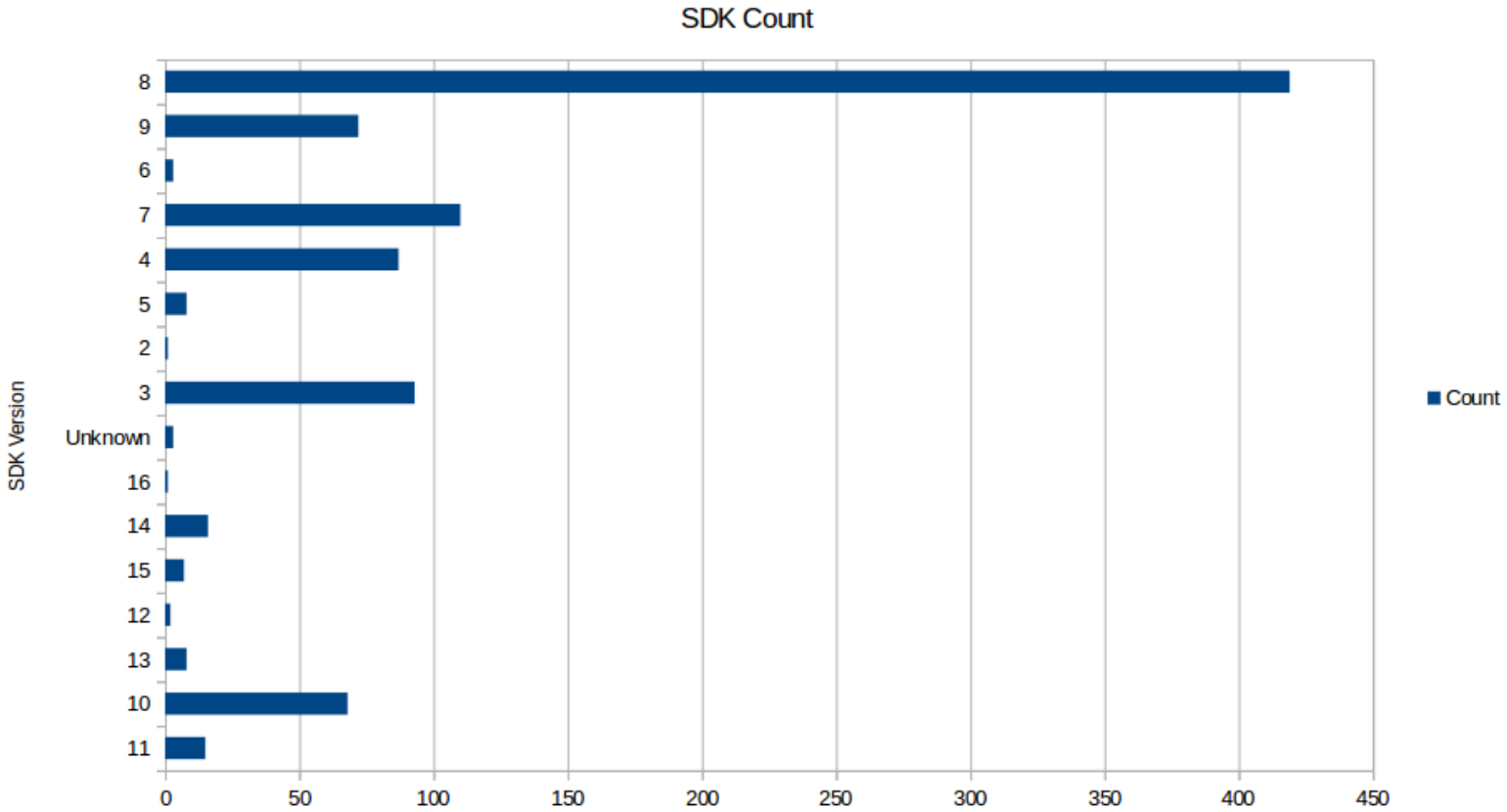


Total Expired Domain Found:

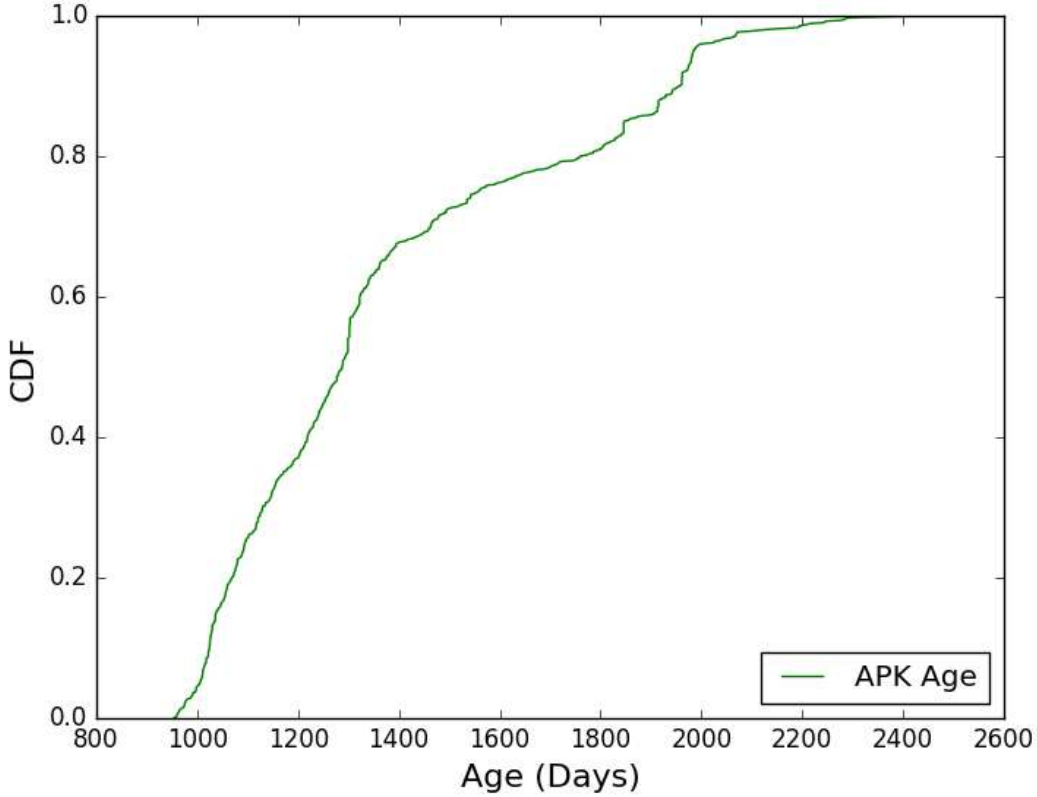
196 + 168 = 364 *Expired Domain*

913 APK

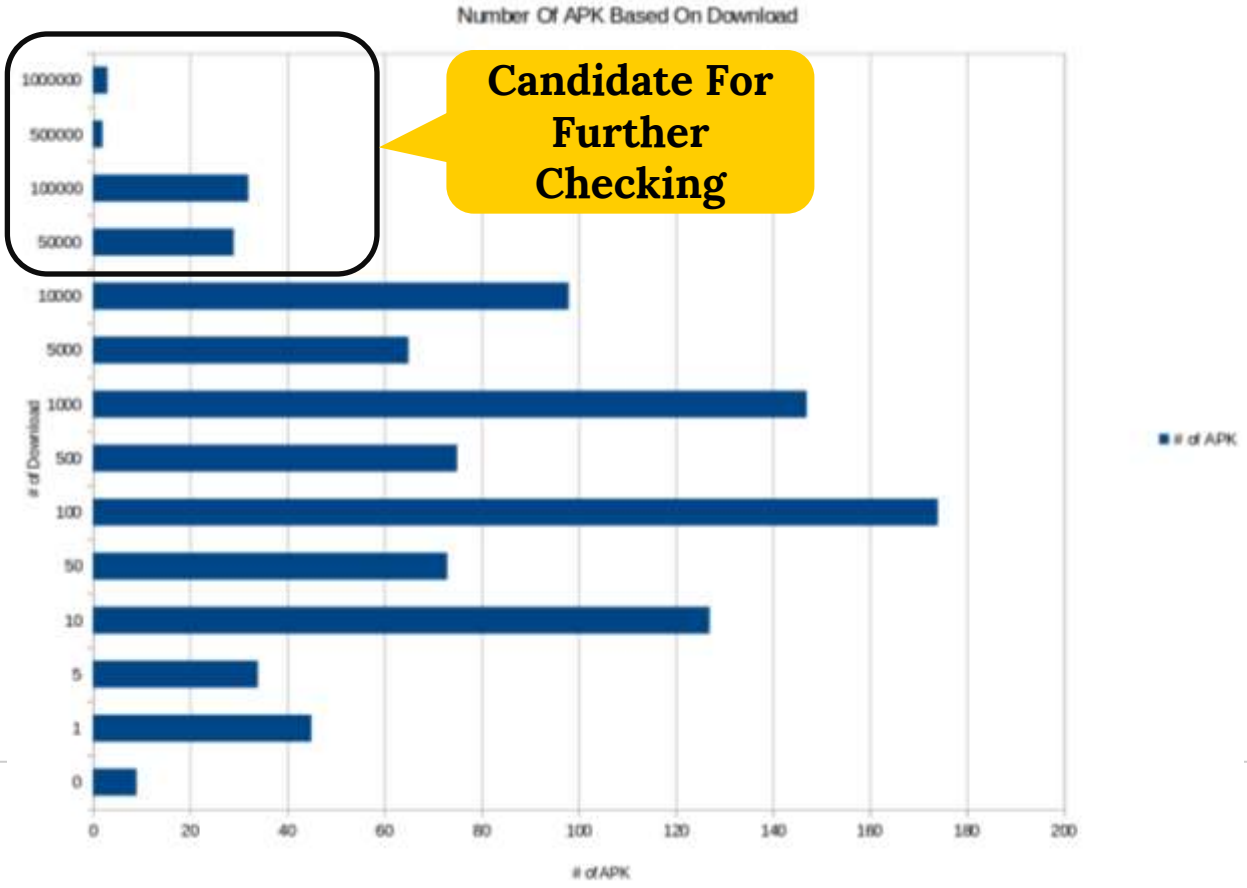
APK Statistic



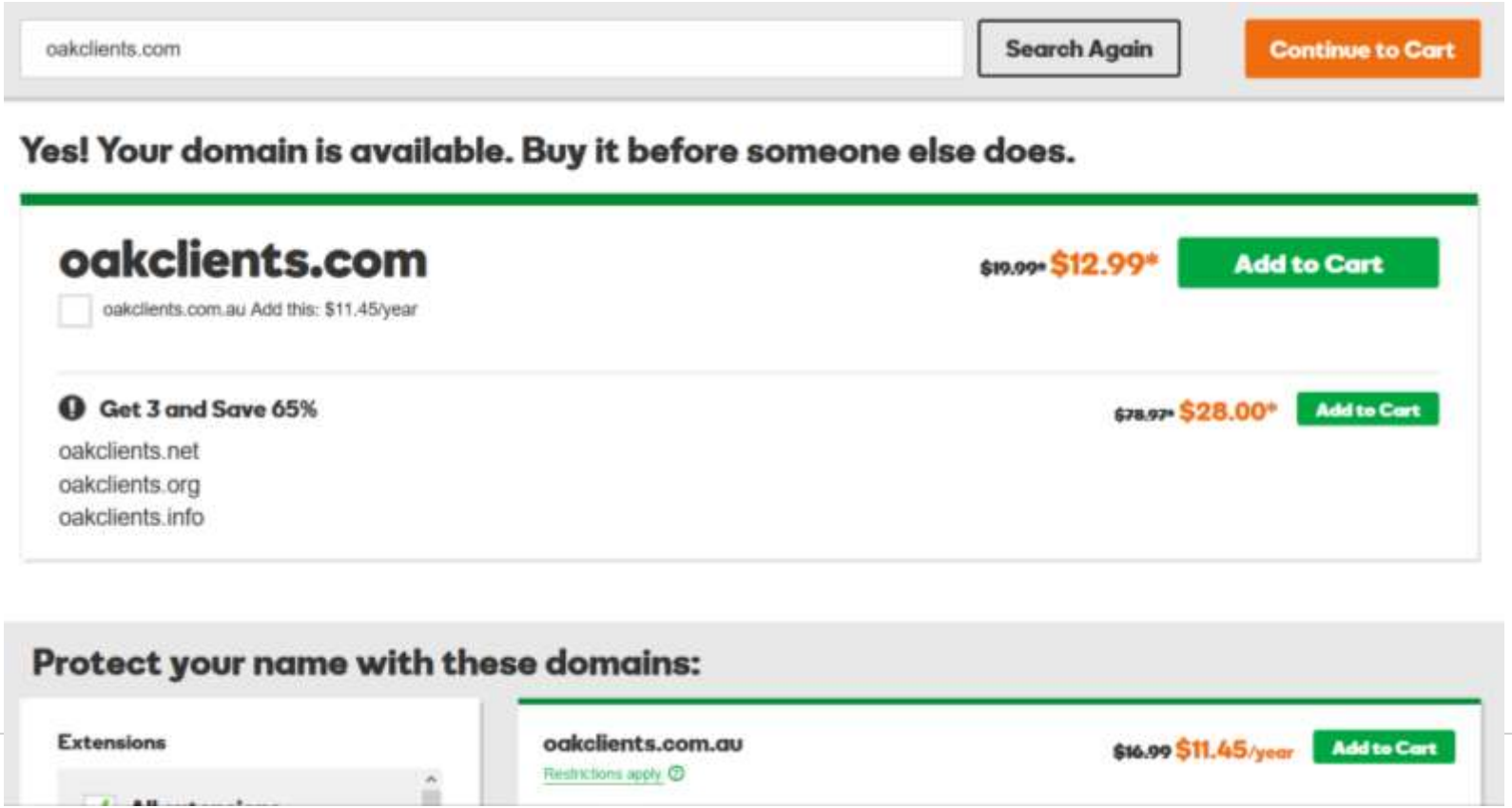
APK Statistic



APK Statistic



About Undetermined Domain

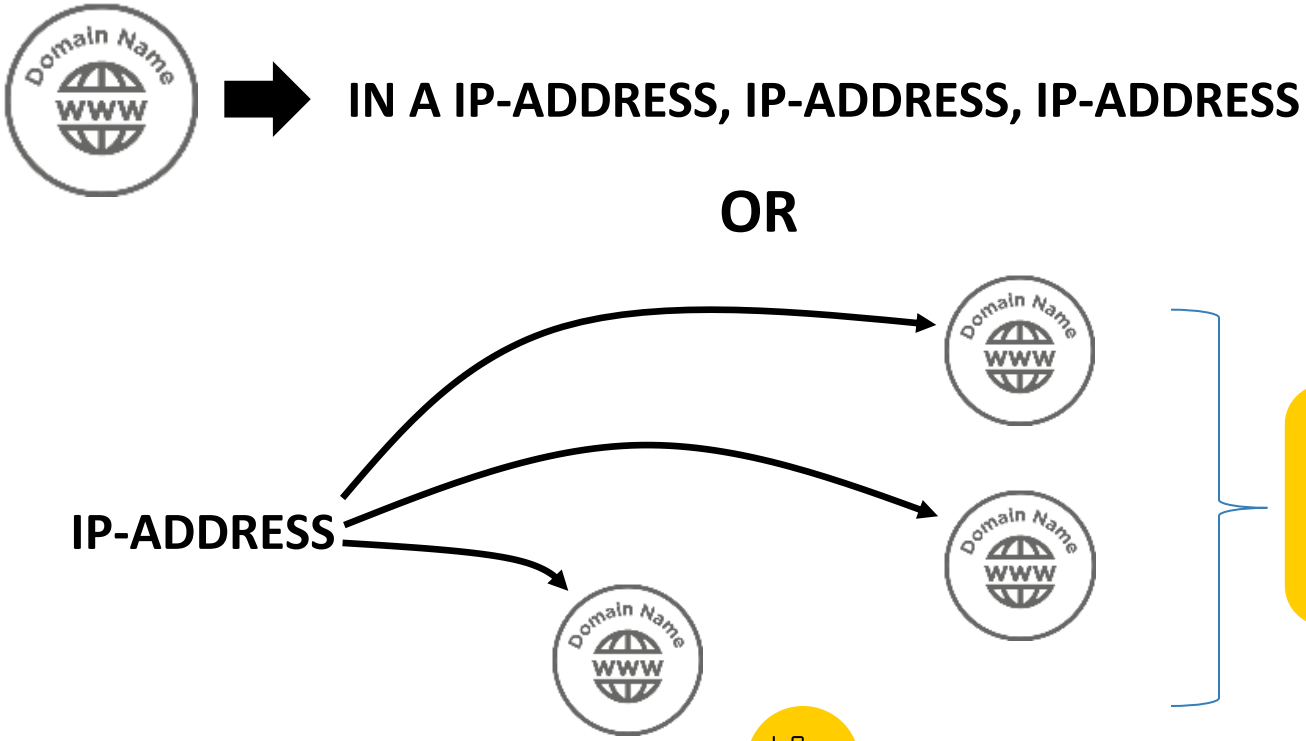


Further Checking of Undetermined Domain

Through Godaddy Domain Availability API
Total : 15889 Domain

Status	# of Domain
Available	2593 Domain
Not Available	10182 Domain
Unsupported TLD	3076 Domain
Invalid Characters	27 Domain
Inappropriate Hyphen	1 Domain
Error Internal	10 Domain

About IP Address



About IP Address

- 35213 Distinct IP Address
- 6332 Unresolved
- 3416 IP is in AWS Range
- 2605 IP is IP for EC2 AWS
- Scan these 2605 for open port 80 and 443
- 330 IP does not have open port 80 and 443
- Domain ? APK ?

Next Step:

- Checking for parked domain (Related Work: Parking Sensors: Analyzing and Detecting Parked Domains, NDSS 2015)

service	Setting	Address
SedoParking	NS	sedoparking.com
InternetTraffic*	NS	internettraffic.com
CashParking*	NS	cashparking.com
Fabulous*	NS	fabulous.com
DomainSponsor	NS	dsredirection.com
Above[1]	NS	above.com
ParkingCrew	NS	parkingcrew.net
	A	62.116.181.25
	CNAME	parkingcrew.net
Skenzo*	NS	ztomy.com
NameDrive	NS	fastpark.net
Voodoo*	NS	voodoo.com
RookMedia	NS	rookdns.com
Bodis	NS	bodis.com
	CNAME	parking.bodis.com
DomainApps	NS	domainapps.com
TrafficZ*	NS	trafficz.com
	A	198.202.142.246
	A	198.202.143.246
TheParkingPlace	NS	pql.net
	Redirect	putoppose.net/d/domain

TABLE I. SUMMARY OF THE OBSERVED PARKING SERVICES TOGETHER WITH THEIR REQUIRED DOMAIN CONFIGURATION. ENTRIES MARKED WITH AN ASTERISK WERE FOUND THROUGH EXTERNAL ANALYSIS.

Next Step:

- Manually checking the usage of the domain in the code
- Checking the availability of the IP in The Cloud
- Related paper : All Your DNS Records Point To Us, CSS 2016
- Tools : http://boto.cloudhackers.com/en/latest/
- Check whether the domain is really contacted by the app by doing dynamic analysis on the app

Thanks!

Discussion