Cyberthreats_
Telefónica

Demographic Analysis of Google Play

07/03/2016

Telefónica

securely powered by ElevenPaths

About the editors

CyberThreats_ Telefónica

The main objective of the Telefónica CyberThreat_ Service is the generation of intelligence adapted to the needs of our customers to counteract those threats that may arise from the digital environment. What differentiates Telefónica from other traditional security services is the capability to integrate, evaluate and transform information and raw data into conclusions and possible future scenarios.

The three pillars supporting the service are:

- Detection
- Analysis and interpretation
- Foresight and anticipation

ElevenPaths

At ElevenPaths we think differently when we talk about security. Led by Chema Alonso, we are a team of experts with concern to rethink the industry and an extensive experience and knowledge in the security sector. We dedicate all our expertise and efforts in creating innovative products so that digital life becomes safer for everyone.

The evolution of security threats in technology is getting increasingly faster and recurring. For that reason, since June 2013, we have established ourselves as a start-up within Telefónica to work in a swift and dynamic manner, and be able to transform the concept of security by anticipating future problems that might affect our identity, privacy and online availability.

With headquarters in Spain, we are also present in the UK, the United States, Brazil, Argentina, and Colombia.

Executive summary

The sample carried out in the beginning of February 2016, shows that Tacyt had dissected a total of 3,365,527 applications from the Google Play Store, of which only 2,438,864 remained available for download on the market.

According to the email address used by developers at the Google Play Store (developerEmail), Tacyt has information on 678,328 different developers. About 44% of email addresses present in Google Play Store are from the "gmail.com" domain.

Google requires developers to sign all their applications prior to being published in the Google Play Store. This certificate is used to identify the author of the application. The total number of different certificates found by Tacyt has been 805,731. Even though the vast majority of certificates found are associated with a single email address, there are exceptions. Even one certificate related to more than ten thousand different email addresses has been found.

Sharing the same certificate among several developers is not a recommended best practice from a security standpoint, since it could compromise the apps' update process or the information they handle. Of the 805,731 certificates (certificateFingerprint) known by Tacyt, 761,389 are associated with a single developer email address (developerEmail). The rest is used by two or more different developer email addresses to sign their applications.

Table of contents

Introduction

Demography, from the Greek *demos* (people) and *graphia* (description of) is defined as the statistical study of a human community, referred to a specific period or to its evolution[1].

In this regard, the report aims to study the population of developers and applications in the Google Play Store in early February 2016, to determine its size, structure, evolution and general characteristics from a quantitative point of view.

Tacyt has been used as a source of information. Tacyt is an innovative cyber-intelligence tool that monitors, stores, analyses, correlates and classifies millions of mobile apps thanks to its big data technology, adding thousands of new applications every day[2].

[1] http://www.etymonline.com/index.php?term=demography
[2] https://www.elevenpaths.com/technology/tacyt/index.html

Basic demographic indicators

There are several sources of information on the Internet, providing a collection of basic indicators with the historical evolution of the number of applications available in the Google Play Store.

"Statista", a portal specialised in statistics, indicated that in November 2015 there were 1,800,000 apps in the Google Play Store[3]:

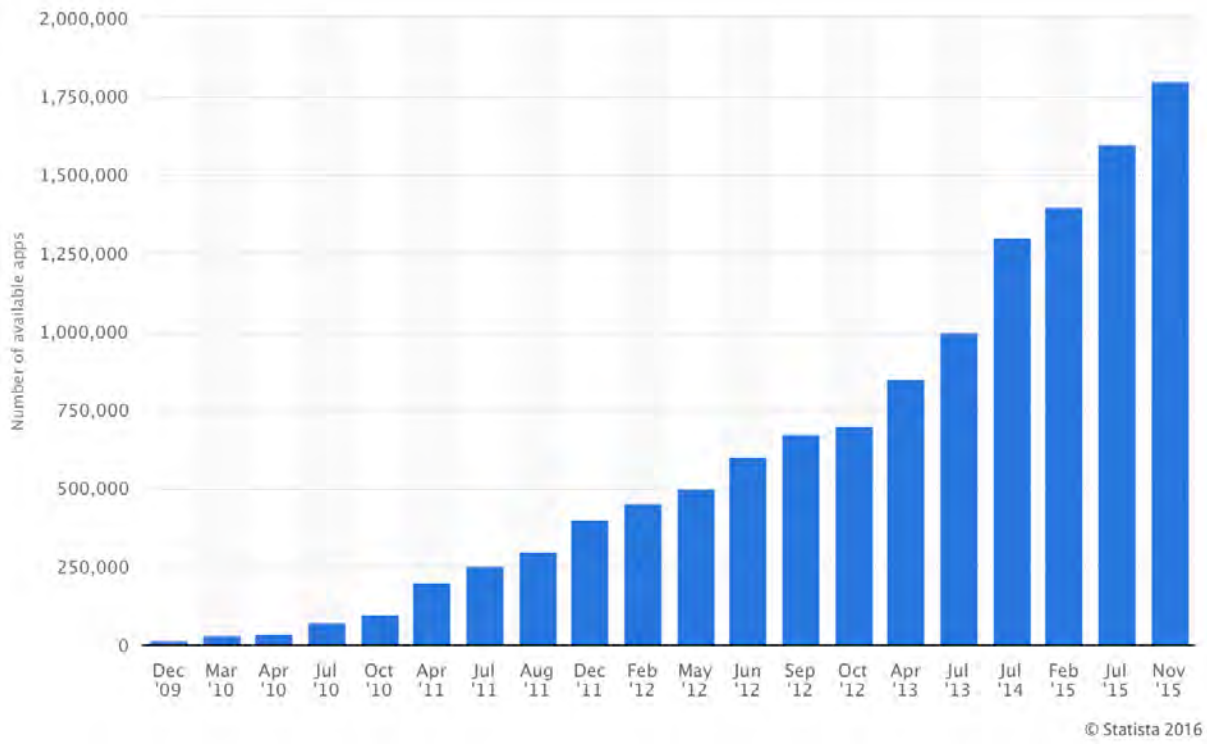


Figure 1. Number of apps in the Google Play Store (Statista Dec 2009 - Nov 2015)

"AppBrain", the Android apps directory, also provides information on the number of applications available in the Google Play Store. Furthermore, it is also possible to find additional information such as: a monthly number of new apps, the distribution of

[3] http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

apps' ratings, downloads, classification of apps according to their quality (low quality vs. regular), categories in which they are included, most popular applications, etc. [4]

In early February 2016, "AppBrain" indicated there were about 2 million apps available in the Google Play Store.

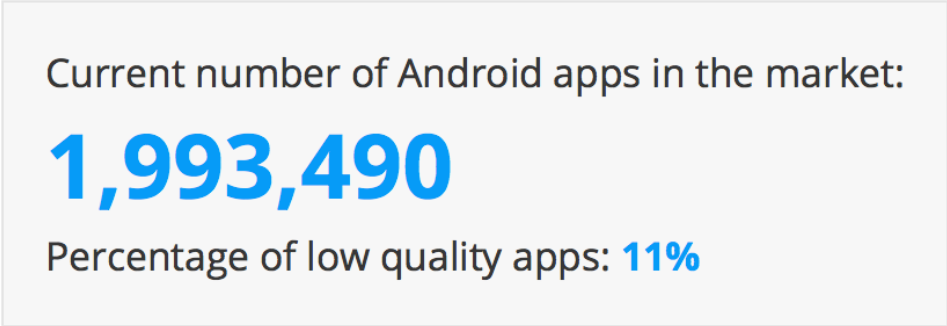


Figure 2. Number of apps available in the Google Play Store (AppBrain Stats February 2016).

Almost half a million more than the ones it recorded one year ago:

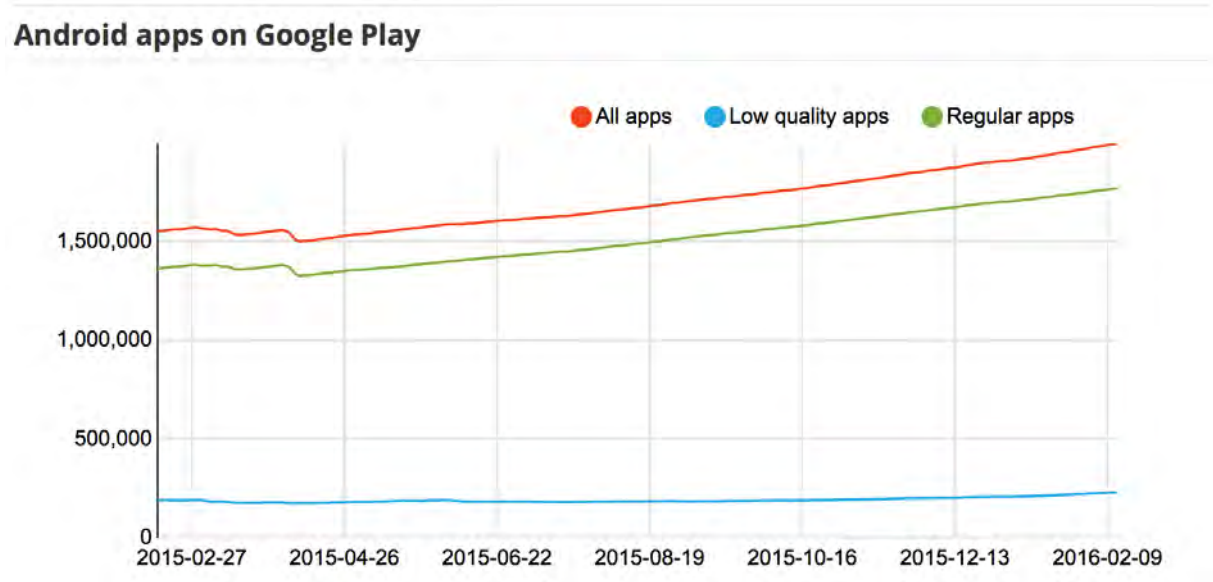


Figure 3. Number of apps available in the Google Play Store (AppBrain Stats February 2015 - February 2016).

[4] http://www.appbrain.com/stats/number-of-android-apps

Lastly, using "App Annie" as source, in mid-February, the number of available apps stood at 2,344,363[5] in the Google Play Store:

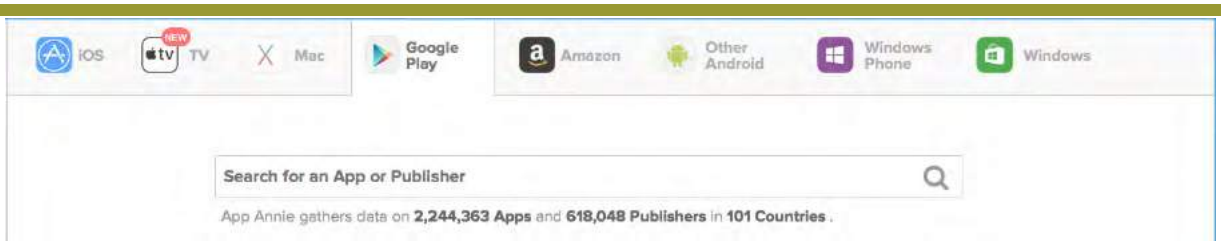


Figure 4. Number of apps available in the Google Play Store (App Annie Stats February 2016).

This source, unlike AppBrain, provides information on the number of developers (publishers) and places it in 618,048 distributed across more than 100 countries.

In order to extract a more complete information concerning developers, it is necessary to resort to the Tacyt source. By analysing the information available on Tacyt associated with Google Play Store, we were able to obtain the following data:

Table I: Information available on Tacyt about Google Play Store (February 2016)

What does Tacyt know about Google Play Store?	Total
Number of applications known by Tacyt	3,365,527
Number of different applications (packageName)	2,316,838
Total applications removed (no longer available on Google Play)	926,663
Number of single email addresses associated with developers	678,328
Number of different developer names	539,468
Number of single certificates (certificateFingerprint)	805,731
Number of different public keys	805,624

Key Topic: high mortality rate of apps

The sampling carried out in early February 2016, shows that Tacyt keeps a total of 3,365,527 applications from the Google Play Store, of which only 2,438,864 are different applications (different packageName).

In addition, Tacyt has stored about one million apps that are no longer available for download from the Google Play Store (either because the developer updated the

[5] https://www.appannie.com/search/?vertical=apps&market=google-play

version of their app and eliminated the previous ones, or because they decided to remove it or because it was Google Play who eliminated it from their Store).

Key Topic: it is difficult to determine the exact number of single developers

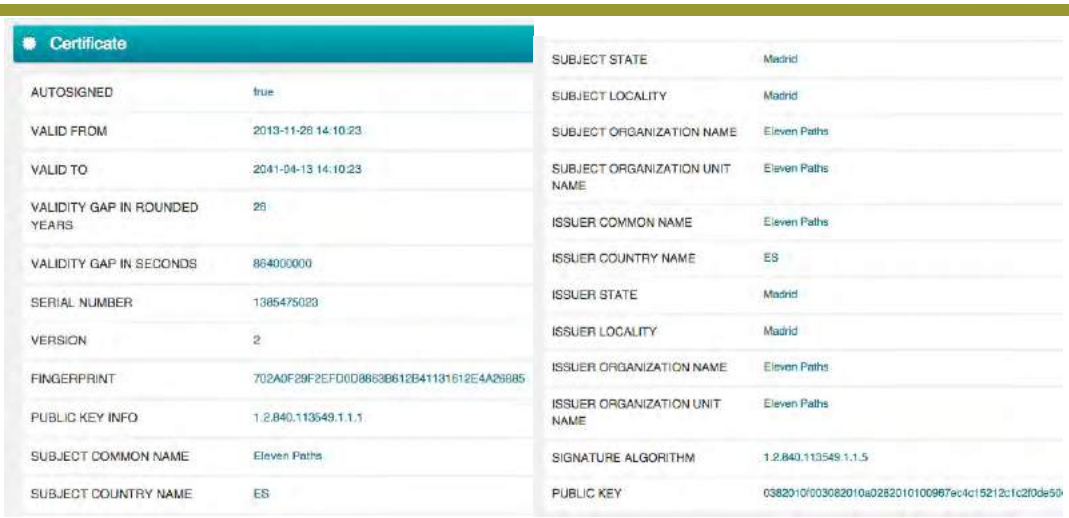
According to the email address used by the developer in the Google Play Store (developerEmail), Tacyt has information on 678,328 different developers. This order of magnitude coincides with what App Annie was reporting, being able to match the deviation between the numbers provided by both sources to the freshness of the information, which is greater in the case of Tacyt.

Figure 5. Detailed information available on Tacyt associated to the developer example

Focusing on the data provided by Tacyt, it is interesting to dwell on the comparison of some values. For example, according to the different number of developer names obtained (developerName) versus the number of certificates used to sign the apps, several hypotheses can be raised:

- The same developer might be using multiple email addresses.
- The developer might be identifying themselves through various developer names.
- They might be using different certificates to sign the different apps they develop.

Throughout this report it will be shown that this results in a common practice among developers, and that they can change name, certificate or email addresses regularly in order to try to disguise or diversify the identity under which they publish. Unfortunately, with the information that can be collected through direct consultation of Google Play, it is impossible to reconstruct the timeline in which these practices occur.



Certificate

AUTOSIGNED	true
VALID FROM	2013-11-28 14:10:23
VALID TO	2041-04-13 14:10:23
VALIDITY GAP IN ROUNDED YEARS	28
VALIDITY GAP IN SECONDS	884000000
SERIAL NUMBER	1385475023
VERSION	2
FINGERPRINT	702A0F29F2EFD0D8663B612B41131612E4A26885
PUBLIC KEY INFO	1.2.840.113549.1.1.1
SUBJECT COMMON NAME	Eleven Paths
SUBJECT COUNTRY NAME	ES
SUBJECT STATE	Madrid
SUBJECT LOCALITY	Madrid
SUBJECT ORGANIZATION NAME	Eleven Paths
SUBJECT ORGANIZATION UNIT NAME	Eleven Paths
ISSUER COMMON NAME	Eleven Paths
ISSUER COUNTRY NAME	ES
ISSUER STATE	Madrid
ISSUER LOCALITY	Madrid
ISSUER ORGANIZATION NAME	Eleven Paths
ISSUER ORGANIZATION UNIT NAME	Eleven Paths
SIGNATURE ALGORITHM	1.2.840.113549.1.1.5
PUBLIC KEY	0382010f003082010a0282010100967ec4c15212c1c2f0de50

Figure 6. Information in Tacyt associated with the certificate with which the app is signed

Population analysis

By analysing 678,328 email addresses associated with developers that Tacyt managed to find on Google Play Store, is easy to determine what are the most common domains and nicknames appearing in the developerEmail (nickname@domain) field.

Table II: The Top 10 domains used as developer email (February 2016)

Developer Email Domain	No. of Emails
gmail.com	296.917
hotmail.com	8.883
yahoo.com	5.655
naver.com	4.258
googlemail.com	3.077
outlook.com	2.504
mail.ru	1.326
live.com	1.090
163.com	1.050
hanmail.net	902

Table III: The Top 10 nicknames used as developer email (February 2016)

Developer Email nickname	No. of Emails
info	66,430
support	35,141
contact	12,301
android	6,873
apps	6,103
contact	4,178
app	3,076
sales	2,826
webmaster	2,798
hello	2,654

About 44% of email addresses present in the Google Play Store belong to the "gmail.com" domain. In total, there are more than 286,000 different domains present in the developerEmail. The most common correspond to free email providers.

As for nicknames, the most common ones are generic names of support, information or contact. The word "*contato*" in Brazilian Portuguese is highlighted within the Top 10. The rest tend to be terms in English.

According to the TLDs associated to the domains found in email addresses, there are more than 480 different TLDs, almost 60% of the developerEmail use a ".com" email address:

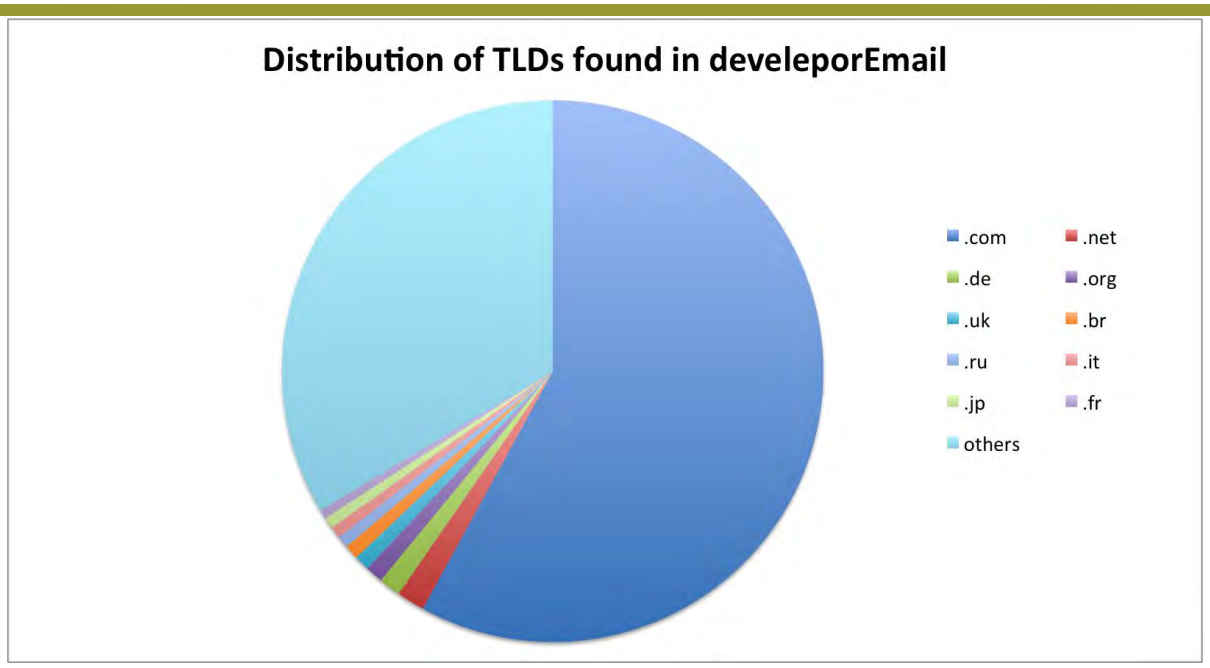


Figure 7. Distribution of TLDs found in email addresses (developerEmail)

With regard to the ".es" TLD, the most commonly used domains are shown below, as well as the most common nicknames.

Table IV: The Top 10 ".es" domains used as developer email (February 2016)

Developer Email Domain	No. of Emails
yahoo.es	140
hotmail.es	89
outlook.es	38
juntadeandalucia.es	18
movistar.es	10
outlook.com	9
gmail.es	7
xunta.es	7
ivhusa.es	7
wke.es	7
rba.es	7
orange.es	7
chorrasoft.es	7

Table V: The Top 10 nicknames used as developer email (February 2016)

Developer Email nickname	No. of Emails
info	1,012
contact	101
support	95
apps	46
android	46
support	42
app	36
admin	36
hi	34
commercial	27

There are 2,941 different ".es" domains used by 3,657 ".es" different developer email addresses.

The following table shows the most common developer names (developerName) found, taking into account the number of apps uploaded. The first three are Chinese names (the table includes a translation using Google Translate):

Table VI: Top 10 developer names with the highest number of applications on Google Play (February 2016)

Developer Name	No. of apps
천지인운세 *(Tenchijin Horoscopes)*	7,342
길선백 *(Gilseon back)*	7,102
학교기업 *(School now)*	6,083
Nobex Technologies	4,314
한겨레신문사 *(Hankyoreh newspaper)*	3,844
Subsplash Consulting	3,375
Shopgate GmbH	2,576
대구대앱창작터 *(Daegu app from creation)*	2,535
CrowdCompass by Cvent	2,333
MagazineCloner.com	2,170

Similarly, by considering the total number of apps uploaded (including those currently available as well as the non-available ones), the developer email ranking (developerEmail) on Google Play Store can also be obtained.

Table VII: Top 10 email addresses with the highest number of apps uploaded to Google Play (February 2016)

developerEmail	No. of apps
customer.services@tobit.com	12,706
drsupport@nobexinc.com	4,315
support@crowdcompass.com	3,445
sorokin9910071559@gmail.com	3,153
help@pocketmags.com	2,670
support@thechurchapp.org	2,554
support@shopgate.com	2,534
admin@skoolbag.com.au	2,140

developerEmail	No. of apps
themesonlyex@gmail.com	2,112
support@reverbnation.com	1,896

In the top 10, there are email addresses associated with companies involved in software development: "Tobit.Software", "CrowdCompass" and "The Church App" among others.

Let us focus now on the developer names (developerName) with which the most used email accounts are related.

The "customer.services@tobil.com" email address is associated with 1,385 different developer names. The majority tend to explicitly contain the string associated with the "Tobit.Software" company name. But if we discard the developer names in which "Tobit.Software" appears, we find a full listing of companies and limited liability companies (GmbH), which have entrusted the development of its mobile application to "Tobit.Software". The detail of the information retrieved is shown in the following tables:

Table VIII: Top 10 developerName associated with the "customer.services@tobit.com" email address.

Developer name	No. of apps
Tobit.Software	834
Tobit Software AG	487
Tobit.Software GER1	413
Tobit.Software GER2	393
Tobit.Software GER3	354
Tobit.Software GER4	345
Tobit.Software GER5	307
Tobit.Software GER6	286
Tobit.Software GER7	266
Tobit.Software GER8	264

Table IX: The most common developerName associated with "customer.services@tobit.com" in which the "Tobit.Software" string does not appear.

Developer name	No. of apps
APPJETZT - IT-Center Engels	53
Experten Service Point GmbH	52
plusO®	48
Buschkamp Consulting	48
Wellhausen & Marquardt Medien	47
Stolz Computertechnik GmbH	43
Mindtraffic GmbH Fred Posny	43
dunnet.de	35
Groth	34
Christian Süß	24

The "drsupport@nobexinc.com" email address uses only two different developer names, both related to mobile apps for the tuning of radio stations.

Table X: Developer names behind the "drsupport@nobexinc.com" email

Name of developer used	No. of apps
Nobex Technologies	4,314
Rumsey Retro Radio AM 1580	1

We find 11 different developer names for “support@crowdcompass.com”

Table XI: Developer names behind the “support@crowdcompass.com” email

Name of developer used	No. of apps
CrowdCompass by Cvent	2,333
CrowdCompass Inc	1,083
Cvent - Portland	12
American Bar Association	7
Aetna Life Insurance Company	3
Aetna	2
Viewpoint Construction Software	1
Intel Corporation	1
CrowdTorch	1
Agilysys NV	1
Academy of Management	1

In the case of "sorokin9910071559@gmail.com", only two different developer names are used.

Table XII: Developer names behind the “sorokin9910071559@gmail.com” email

Developer name used	No. of apps
Andrey Sorokin	2,148
iniCall.com	1,005

Lastly, we again find eleven different developer names for "help@pocketmags.com".

Table XIII: Developer names behind the "help@pocketmags.com" email

Name of developer used	No. of apps
MagazineCloner.com	2,168
Pocketmags.com	399
KHL Group LLP	37
Pocketmags.com.au	33
Future Publishing Ltd	13
Newsquest Specialist Media Ltd	7
Key Publishing Limited	6
UTV Media plc	3
ILoveMagazines.com.au	2
Reader's Digest UK	1
mobile_apps_team	1

Key Topic: the email addresses used in the Google Play Store do not have to be registered

Behind a certain developerEmail, one or more individuals can be found, or software development companies that use the same email to upload a number of apps to Google Play Store which can be associated with multiple services and various companies.

By analysing the different developer names, it is possible to determine the client portfolio of companies dedicated to the development of apps. In the event that an attacker would find a vulnerability in one of these applications, they could easily list the set of applications developed by the same team and analyse whether they are also vulnerable or not.

This has already been the case in the past with, for example, AppsGeyser, an applications creator with just a few clicks, which was turning off the checking of SSL certificates in their applications. An attacker on the same local network as a user who utilises these applications, will be able to inject any page while browsing from the affected apps, or view and modify websites that should be protected[6].

[6] http://blog.elevenpaths.com/2014/12/5500-apps-potentially-vulnerable-to-man.html

Going back to the top of the email addresses associated with the developers who have uploaded the highest number of apps to Google Play Store, we can examine the number of single apps.

The following table shows how while some developers, namely support@reverbnation.com, rarely update the apps they upload to the Google Play Store, others, such as "help@pocketmags.com" or "themesonlyex@gmail.com" have updated three times each app on average.

Table XIV: Comparison on apps uploaded to Google Play vs single apps for the top 10 email addresses with more applications on Google Play (February 2016)

developer Email	No. of apps	No. of single apps
customer.services@tobit.com	12,706	8,235
drsupport@nobexinc.com	4,315	1,951
support@crowdcompass.com	3,445	2,291
sorokin9910071559@gmail.com	3,153	1,044
help@pocketmags.com	2,670	680
support@thechurchapp.org	2,554	1,171
support@shopgate.com	2,534	1,455
admin@skoolbag.com.au	2,140	1,549
themesonlyex@gmail.com	2,112	678
support@reverbnation.com	1,896	1,886

It is also possible to display information on applications (packageName) that received the most updates since 2014:

Table XV: The Top 10 apps with more versions (February 2016)

Package name	No. of versions
com.dwdesign.tweetings	81
wp.wpbeta	61
com.komado.Odyssey.com.nifty.homepage2	59
com.mad.tihh.mixtapes	57
com.tavla5	55
com.ninefolders.hd3	54
com.borisov.strelokpro	52
com.vertumus.cryten	51
com.imo.android.imoimbeta	50
com.gau.go.launcherex	48

Tacyt has detected 81 updates for the "Tweetings for Twitter" application, which means an average of more than four monthly updates.

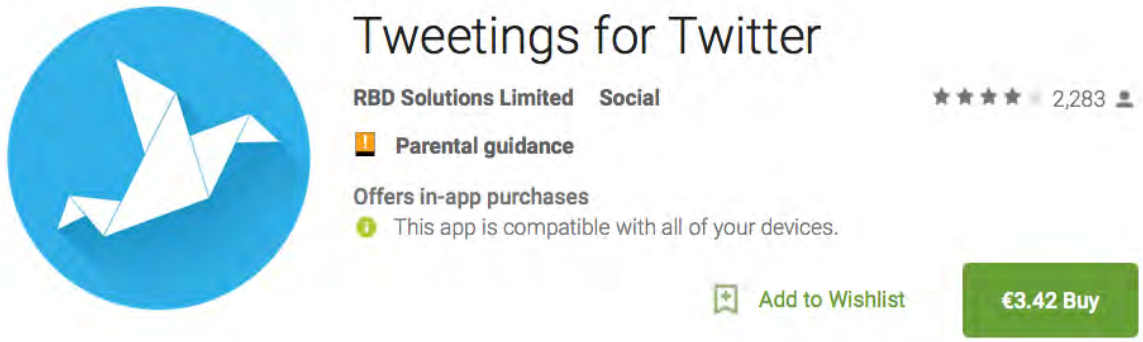


Figure 8. Details of the "Tweetings for Twitter" app in the Google Play Store

According to the number of single apps in the Google Play Store, the top 10 of developerEmail would be the one showed on the following table:

Table XVI: The Top 10 email addresses with the highest number of applications uploaded to Google Play (February 2016)

developer Email	No. of apps
customer.services@tobit.com	8,235
support@crowdcompass.com	2,291
drsupport@nobexinc.com	1,951
support@reverbnation.com	1,886
scscreations@gmail.com	1,665
help@brainpub.co.kr	1,615
admin@skoolbag.com.au	1,549
carismaeo@gmail.com	1,525
support@shopgate.com	1,455
help@epyrus.com	1,423

It is also interesting to analyse how many different developer names (developerName) there are behind each developer email (developerEmail). The following table lists the email addresses using a larger number of different developer names:

Table XVII: Top 10 developerEmail using the highest number of different developer names (February 2016)

Developer Email	No. of developer Names
customer.services@tobit.com	1,385
support@userfriendlymedia.com	413
android@doubledutch.me	111
info@appmachine.com	86
support@vbulletin.com	74
android@doapps.com	51
support@uppsite.com	45
support@gmail.com	31
info@gmail.com	28
product@nine-yi.com	26

Performing the same analysis for the developer emails that use the ".es" TLD:

Table XVIII: Top 10 developerEmail (.es) using the highest number of different developer names (February 2016)

Developer Email	No. of emails
info@pressmatic.es	7
apps@valenapps.es	6
moviles@unidadeditorial.es	4
kai.v@hotmail.es	3
internet@mpib.es	3
info@innovationstudio.es	3
info@dfcsolutions.es	3
info@applinet.es	3
apps@intelectiva.es	3
info@pressmatic.es	7

Below are the developer names used by the two email addresses that spearhead the previous table:

Table XIX: Developer names behind the "info@pressmatic.es" email

Name of developer used	No. of apps
Centro hospitalario Chuac	1
CIRUBUCA	1
Editorial 5150	1
Infolibre	1
itbook	1
Mikel Areitioaurtena	1
PressMatic	1

Table XX: Developer names behind the "apps@valenapps.es" email

Developer name used	No. of apps
Fun Apps	1
Colorea Valencia	1
Sentences in Spanish	1
Funny Smartphone Kids	1
Kid Games	1
Messages Apps	1

Certificate analysis

Google requires developers to sign all their applications prior to being published in the Google Play Store. This certificate is used to identify the author of the application. According to the official Google documentation[7]:

> *Signing Your Applications.*
>
> *Android requires that all apps be digitally signed with a certificate before they can be installed. Android uses this certificate to identify the author of an app, and the certificate does not need to be signed by a certificate authority. Android apps often use self-signed certificates. The app developer holds the certificate's private key.*
>
> …
>
> *Signing Considerations*
>
> …
>
> *If you plan to support upgrades for an app, ensure that your key has a validity period that exceeds the expected lifespan of that app. A validity period of 25 years or more is recommended. When your key's validity period expires, users will no longer be able to seamlessly upgrade to new versions of your application.*

Certificates do not have to be generated by a certification authority, so they can be self-signed. Google indicates that the validity of the certificate should be of at least 25 years, since its use is essential in the apps updating process. It is the responsibility of the developer to make sure the private key remains secure.

As mentioned at the beginning of this document, Tacyt is able to dissect the information associated with the certificate with which the developer signs each app of the Google Play Store, extracting the entities displayed in Figure 6.

The total number of public keys found in the Google Play Store amount to 805,624, which generate a total of 805,731 different certificates (each of these certificates has a unique certificateFingerprint).

Only three three public keys were found to be used in generating more than a single certificate (certificateFingerprint):

[7] http://developer.android.com/tools/publishing/app-signing.html

Table XXI: Public keys (first characters of the certificatePublicKey) that generate multiple certificates

Public key	No. of different certificates
03818d00308189028181009 6f729949a260c7d02275ac68c93b53cbad4cb53...	101
0382010f003082010a028201010090b0b1ebbe3aa1bf4673aef5d8ee09139e...	7
03818d0030818902818100ad04a06c0815469c380d62afd6babe78720c5cdc...	2

This behaviour in itself constitutes a singularity in the typical behaviour of the system's users. A singularity is no more than a feature or detail that distinguishes one element from others of the same kind. The importance of these singularities lies in the empirical fact that normally they constitute evidence worth investigating.

Key Topic: singularities represent evidence in order to carry out investigations

Below are shown the top 10 of both public keys based on the number of apps uploaded to Google Play Store and signed with them.

Table XXII: Top 10 certificatePublicKey (February 2016)

Public key used in the certificate	No.of apps
03818d0030818902818100d6198c6f4685cfcd4435c0efe9f0...	52,129
0382010f003082010a02820101009bbc9e38e883c581fc67dc...	32,988
03818d00308189028181009 38cd7ea321af0ef3272fd25d37a...	26,262
0382010f003082010a02820101009ff1622bc9ffc064949cdc...	16,865
03818d0030818902818100b5002784be33acb7a2c03af22989...	13,467
0382010f003082010a0282010100d818a34292de48821d38e7...	9,548
03818d00308189028181009 40e7dcb09f198ef35ecae158418...	8,877
0382010f003082010a0282010100dbed9654b7fc556340c1ad...	7,392
03818d0030818902818100864 2b807daef2f28b8ef6badf474...	6,871
03818d0030818902818100a46d9cb660fc2abb60d6459c0e76...	5,255

There is an interconnected relation between public keys and certificates of the two previous tables (each public key in the table is used to generate one and only one

certificate, whose mark corresponds to the one appearing in the same position in the table shown below).

Table XXIII: Top 10 certificateFingerprint (February 2016)

Certificate fingerprint	No. of apps
9EDF7FE12ED2A2472FB07DF1E398D1039B9D2F5D	52.129
E44763A669EAE706121C8FC5370094659A310C9B	32.988
29DEDC0E107145215ED6FDC479541F16D164DAAD	26.262
66994CA292C1A37EA9B827731B20CAFE2AB21792	16.865
943BC6E0827F09B050B02830685A76734E566168	13.467
F19AC1C0228C3C3DA455F32665A46A326A8509EB	9.548
813A3AD37D87AA36120DFEC64146C311DB5F4CA9	8.877
8256B772A412EB466DA13B70A50BC9AC94E80243	7.392
B457827C2896E05BBF7FDAA9F4F8A65ED8042CD1	6.871
5C5C56C63B87B3654184C7D0BC86A7205FB2BC1A	5.255

A good practice would be that each developer would generate a single certificate for each app they publish in the Google Play Store. But looking at the previous tables it seems this is not the case (there are far more apps than certificates).

Certificates are a critical component of the security of applications being uploaded to the Google Play Store[8].

> *Signing Considerations*
>
> *You should sign all of your apps with the same certificate throughout the expected lifespan of your applications. There are several reasons why you should do so:*
>
> - *App upgrade: When the system is installing an update to an app, it compares the certificate(s) in the new version with those in the existing version. The system allows the update if the certificates match. If you sign the new version with a different certificate, you must assign a different package name to the application—in this case, the user installs the new version as a completely new application.*
> - *App modularity: Android allows apps signed by the same certificate to run in the same process, if the applications so requests, so that the system treats them as a single application. In this way you can deploy your app in modules, and users can update each of the modules independently.*

[8] http://developer.android.com/tools/publishing/app-signing.html

- *Code/data sharing through permissions: Android provides signature-based permissions enforcement, so that an app can expose functionality to another app that is signed with a specified certificate. By signing multiple apps with the same certificate and using signature-based permissions checks, your apps can share code and data in a secure manner.*

The following image shows the distribution of certificateFingerprint based on the number of apps they sign:

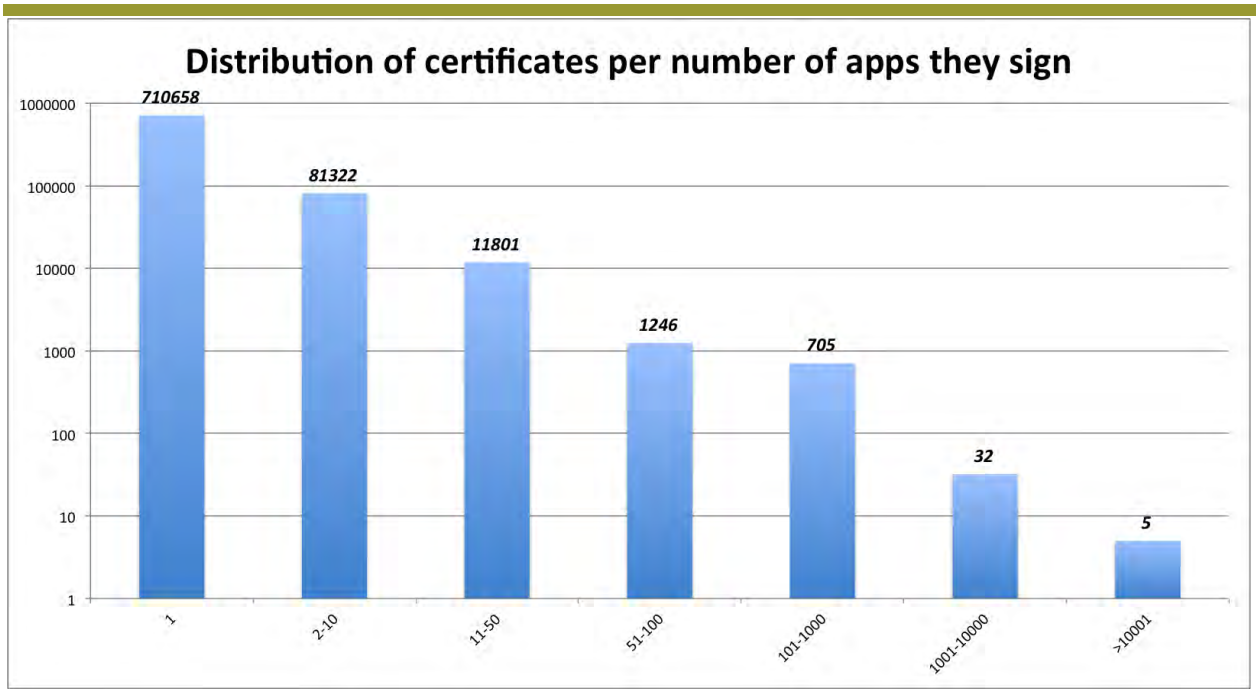


Figure 9. Using certificates to sign one or more apps

In the previous figure, the number of applications sharing the same certificate can be found on the X axis. The Y axis is the number of certificates that fulfils this condition.

Of the 2,316,838 single apps analysed, only 710,658 are signed by a certificate which is not used to sign any other application.

There are five **certificateFingerprint**, each of them used to sign more than 10,000 different apps.

It is easy to find the companies behind these certificates, most of them provide mobile apps development services:

Table XXIV: Top 10 certificateFingerprint - related company

Certificate fingerprint	Company URL
9EDF7FE12ED2A2472FB07DF1E398D1039B9D2F5D	www.appsvolcano.com
E44763A669EAE706121C8FC5370094659A310C9B	www.andromo.com
29DEDC0E107145215ED6FDC479541F16D164DAAD	www.biznessapps.com
66994CA292C1A37EA9B827731B20CAFE2AB21792	www.como.com
943BC6E0827F09B050B02830685A76734E566168	-
F19AC1C0228C3C3DA455F32665A46A326A8509EB	www.mobincube.com
813A3AD37D87AA36120DFEC64146C311DB5F4CA9	ibuildapp.com
8256B772A412EB466DA13B70A50BC9AC94E80243	timmystudios.com
B457827C2896E05BBF7FDAA9F4F8A65ED8042CD1	-
5C5C56C63B87B3654184C7D0BC86A7205FB2BC1A	nobexradio.com

Another interesting approach is to know if several developers may be sharing a same certificate. The following image shows the distribution of certificateFingerprint based on the number of different developer emails (developerEmail) who use it to sign their apps:

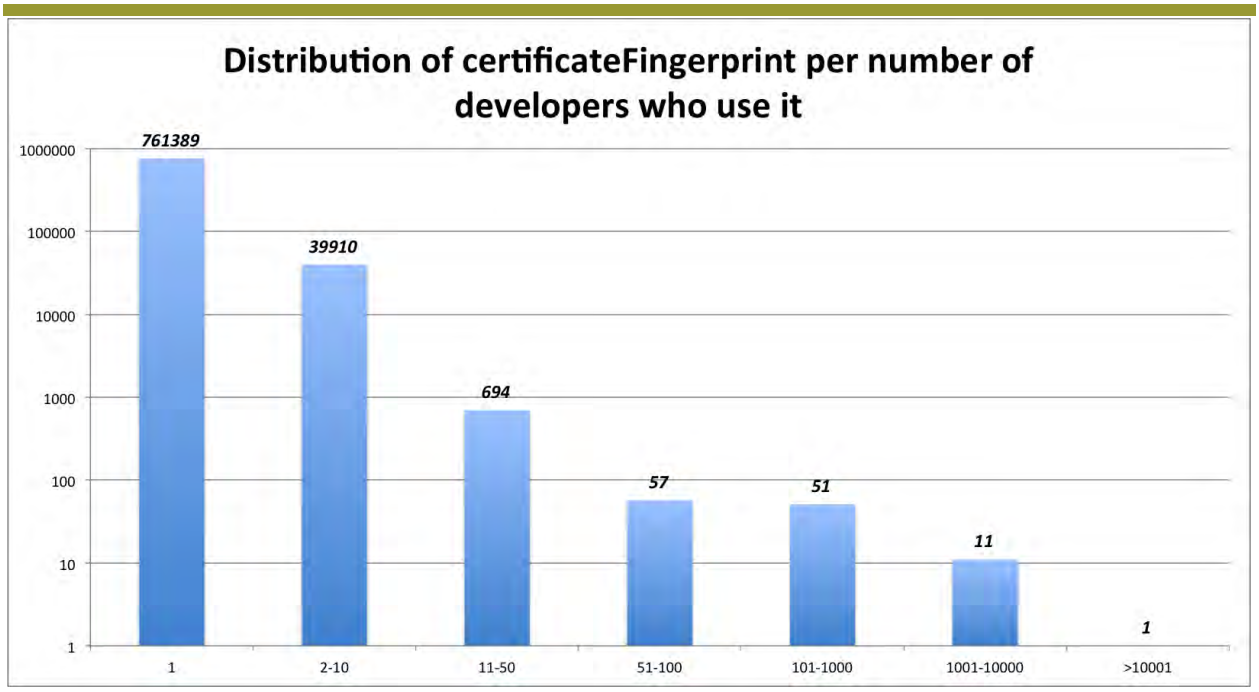


Figure 10. Sharing certificates among developers (developerEmail)

Even though the vast majority of certificates found are associated with a single email address, there are exceptions. Even one certificate related to more than ten thousand different email addresses has been found.

The following table lists the top 10 certificates (certificateFingenprint) which are being used by the largest number of developerEmail.

Table XXV: Top 10 certificateFingerprint associated with more than one email (February 2016)

Fingerprint	emails
66994CA292C1A37EA9B827731B20CAFE2AB21792	10,420
29DEDC0E107145215ED6FDC479541F16D164DAAD	7,237
943BC6E0827F09B050B02830685A76734E566168	5,617
9EDF7FE12ED2A2472FB07DF1E398D1039B9D2F5D	5,361
813A3AD37D87AA36120DFEC64146C311DB5F4CA9	4,758
E44763A669EAE706121C8FC5370094659A310C9B	3,957
F19AC1C0228C3C3DA455F32665A46A326A8509EB	1,736
55A48E1A17A067C7FB22EFB3639558EAC0FC313F	1,452
766D3F4F4876B50894A4EF56FB375C188C15DF96	1,281
7BB234BADDA1FD2CBC65F74983798F9D2A33F556	1,057

Key Threat: it is a bad practice to sign apps associated to different clients or services with the same certificate

Although a company outsources the development of its mobile apps, it is advisable to control the certificate with which the application is signed and manage the upload of the app to the Google Play Store. As a minimum, it should require that the certificate used to sign their application is not shared with any third parties, with whom, the company is perhaps not interested in being involved, or in the worst case, that could access the information the company manages.

We can also analyse how many certificates are associated with each of the addresses found in the Google Play Store.

The following figure, in the X axis, shows the number of certificates related with a specific email address (developerEmail). The Y axis is the number of email addresses that fulfil this condition.

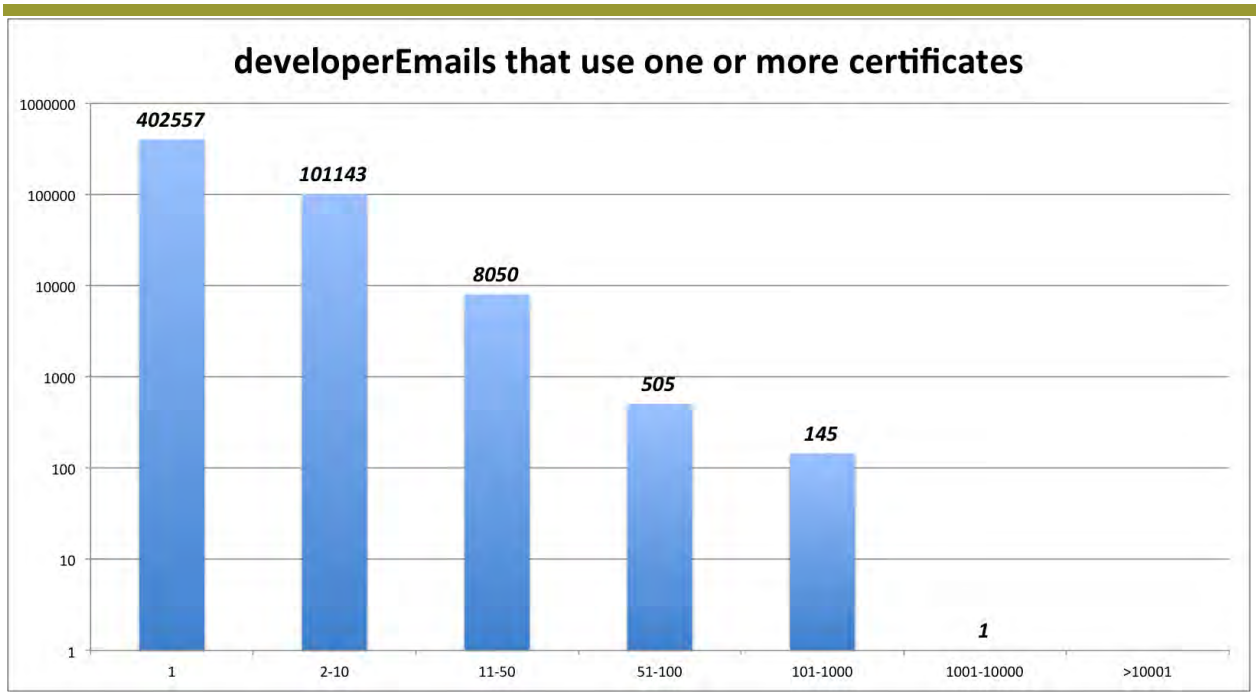


Figure 11. Sharing certificates among developers (developerEmail)

Of the 678,328 known email addresses from Google Play Store, more than three-quarters are associated with a single certificate. However, there are also singularities such as an email address (developerEmail) that uses more than a thousand certificates to sign the different apps it uploads to the Google Play Store.

The top 10 of developerEmail which have used the most certificates is shown below:

Table XXVI: The Top 10 apps with more certificateFingerprint (February 2016)

developerEmail	certificateFingerprint
help.ic@i-connect.co.kr	1,118
GreenCabbagePatch@gmail.com	879
orangecamp0806@gmail.com	673
carismaeo@gmail.com	587
dev@anyline.co.kr	544
help@epyrus.com	521
won@i-connect.co.kr	510
CTSapp@cts.tv	492
accessmobilecwb@gmail.com	440
ndemir.demir@gmail.com	416

Tacyt allows to perform all sorts of statistics with the information it dissects from each one of the certificates. For example, the top 10 names utilised by the user (Issuer Common Name) to generate the certificate is shown below:

Table XXVII: The Top 10 common user names being shown in the certificate (February 2016)

certificateIssuerCommonName	apps
Andrew Vasiliu	52,129
Andromo App	32,988
Unknown	32,800
Andrew Gazdecki	26,262
Conduit Ltd.	16,865
www.appyet.com	15,329
Mobimento Mobile	9,548
Anton	8,967
TMe CEO	7,392
ron maor	5,255

Finally, analysing the validity of the certificates found, as we have discussed above, Google recommends a validity period of at least 25 years[9]:

> *If you plan to support upgrades for an app, ensure that your key has a validity period that exceeds the expected lifespan of that app. A validity period of 25 years or more is recommended. When your key's validity period expires, users will no longer be able to seamlessly upgrade to new versions of your application.*
>
> *If you plan to publish your apps on Google Play, the key you use to sign these apps must have a validity period ending after 22 October 2033. Google Play enforces this requirement to ensure that users can seamlessly upgrade apps when new versions are available.*

The following image shows the distribution of validity periods found on the certificates being analysed.

A significant number of certificates does not meet Google's recommendations/requirements, having a validity period of less than 25 years. 140 certificates were even found to have a validity of 1 year.

[9] http://developer.android.com/tools/publishing/app-signing.html

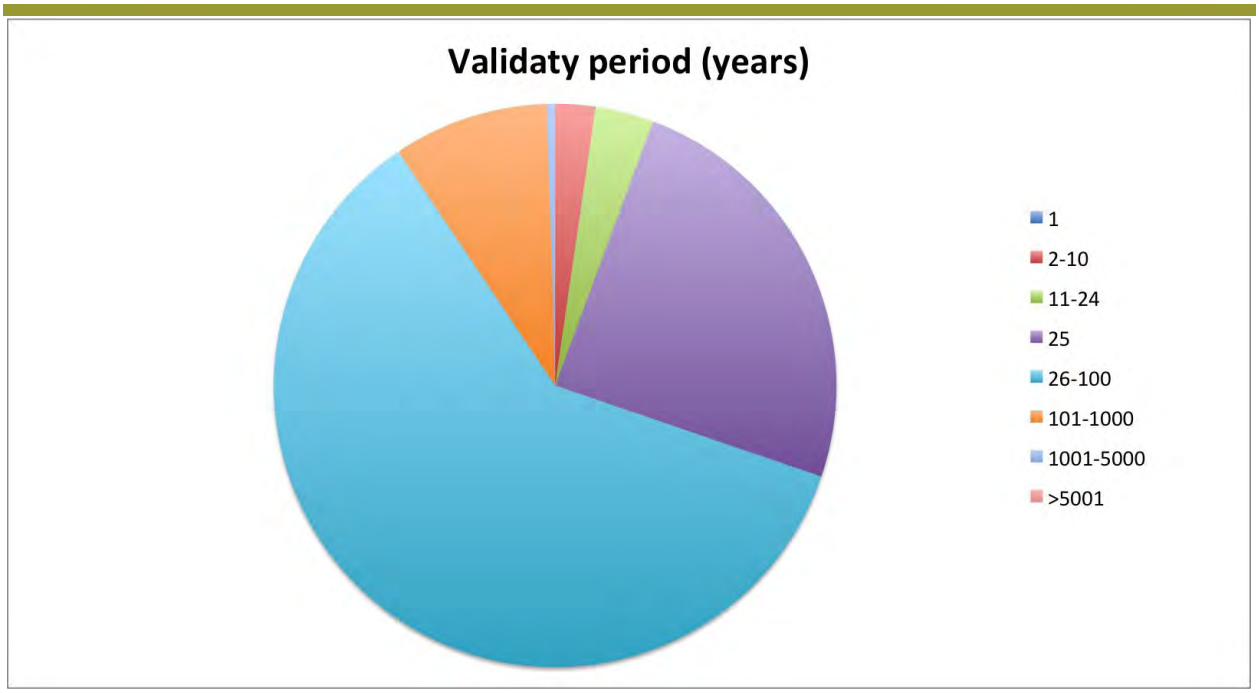


Figure 12. Distribution of certificate validaty period

The following table shows the top 10 most common life spans found in the certificates dissected by Tacyt:

Table XXVIII: The Top 10 most common certificate life spans (February 2016)

Validity (years)	No. of certificates
25	597,405
27	348,051
50	317,467
30	190,940
28	167,215
100	166,800
999	78,699
99	55,491
55	46,678
1000	43,585

Examples of interrelations between the population

A series of graphs are shown below, demonstrating how it is possible to establish relations between different cyber-identities of the Google Play Store, as they share certain resources (singularities).

If we analyse the information Tacyt makes available on the "Warframe Mobile Codex" [10] application:

Figure 13. Details of the app in the Google Play Store

We obtain the following network of relations:

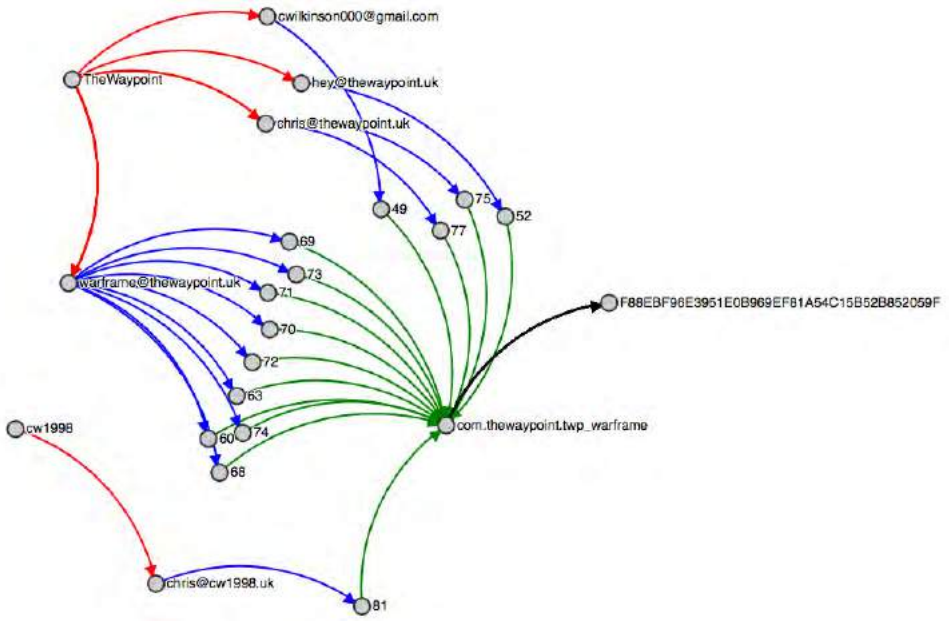


Figure 14. Network of relations among cyber-identities retrieved with Tacyt

[10] https://play.google.com/store/apps/details?id=com.thewaypoint.twp_warframe&hl=en

Tacyt has downloaded 14 different versions of this application from the Google Play Store, the code for each version (versionCode) appears in the previous image next to the balls with incoming blue arrows and outgoing green ones.

The name of the app in Google Play Store (packageName) is "com.thewaypoint.twp_warframe" and is represented in the image above by the ball with incoming green arrows and an outgoing black arrow directed towards the entity associated with the certificate used to sign the app (certificateFingerprint). All versions were signed with the same certificate.

Nevertheless, if we look at the left side of the figure, we can observe how over time, the name of the developer (developerName: balls with outgoing red arrows) and the associated email addresses (developerEmail: balls with incoming red arrows and outgoing blue ones) have changed over time as new versions of the application were being published:

- The developer name used in the first 13 versions was "TheWayPoint" and actually used up to four different emails. Initially an email from Gmail and later three different accounts associated with the "thewaypoint.uk" domain.
- In the latest available version, the developer name changed to "cw1998" and the email associated with the developer has become "chris@cw1998.uk".

Other types of relations that are readily available is from the sharing of certificates (certificateFingerprint) with which several developers sign their apps.

In the following figure, the developer names (developerName) are the origin of the red arrows that end up in the email addresses (developerEMail) used by the developer and with the outgoing blue arrows pointing to the certificate fingerprint (certificateFingerprint) which they used to sign the apps they uploaded to the Google Play Store.

Figure 15. Relations among cyber-identities for using the same certificates

Finally, it is also possible to represent weak relations among cyber-identities using singularities, such as the validity period with which the certificate has been generated (2,873 years in the case shown below):

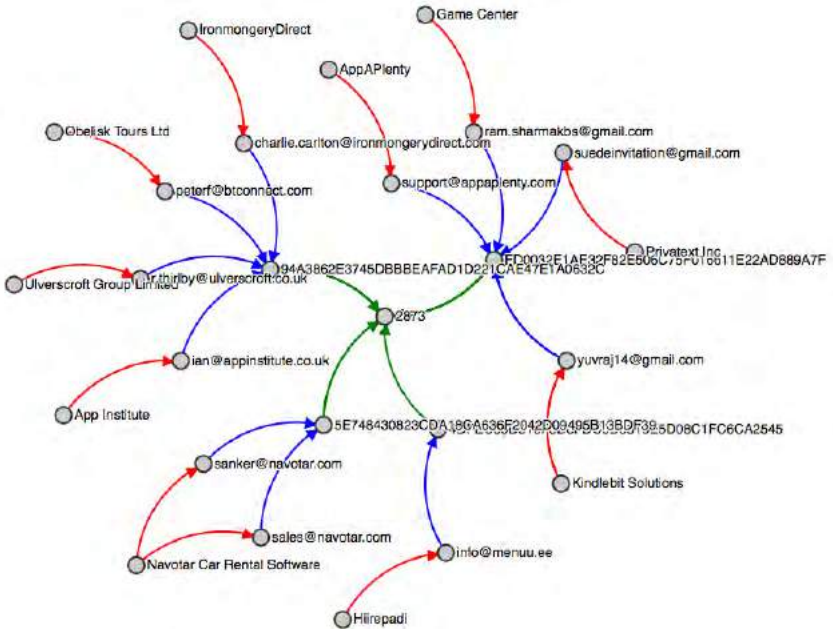


Figure 16. Weak relationships among cyber-identities from a singularity such as the validity period of the certificate used for signing apps

In the previous figure developer names (developerName) are the origin of the red arrows that end up in the email addresses (developerEMail) used by the developer. Blue arrows come out of these addresses pointing towards the certificate fingerprint (certificateFingerprint) which they have used to sign the apps they uploaded to the Google Play Store Finally, a green arrow comes out from each certificateFingerprint heading towards the entity associated with the validity period of the certificate, in this case 2,873 years.

Conclusions

The first conclusion to be drawn from this report is the extremely high variability of the Google Play applications market. By looking through the numbers over the months that Tacyt has been underway, it can be said that the daily average of new applications amounts to 4,500 and it has kept steady with little variation.

It has been verified in this analysis what the trend is in terms of origin of developers and features associated with the alternatives they use in order to be identified in the system. Aside from the statistical interest the information shown in the first part of the document (information of most present TLDs or usernames) possesses, it is intended to highlight what impact these alternatives have when they are related to the use of digital certificates, in the accuracy of identification of developers. In fact, a possible occurrence that may partly explain the causes of this swift and continued growth is the lax policy on the identification of apps developers Google Play has kept ever since its inception. Even though the use of digital certificates for the signing of software should identify the individual or entity behind the software in an unambiguous manner, this report shows through the use of numbers that Google Play facilitates the abuse of this concept and this might lead to situations where such identification becomes compromised.

When a developer (developerEmail) signs their Android application (packageName) with a specific certificate (certificateFingerprint) and uploads it to the Google Play Store, there is no turning back. Neither that application nor its updates may be signed with a different certificate within the Google ecosystem.

Certificates are a critical component of the security of applications being uploaded to the Google Play Store. If a developer wants to use a different certificate to sign the update of one of their applications (for example, because they lost the certificate initially used), they must remove the original application and publish the update as if it were a new application (with a different packageName).

The certificate fingerprint (certificateFingerprint) used to sign an application, in addition to determine who can perform an update to it, it also establishes a relation of trust with those applications that were signed using the same certificate, determining with which others it can share data during its execution.

Android allows applications signed with the same certificate to run in the same process (provided that they also share sharedUserID[11]), thus allowing the system to handle them as a single application (composed by several modules). Besides, it also allows the sharing of data and functionalities safely between applications (the permission verification is based on the certificate with which the applications are signed).

From the analysis performed, it is possible to identify several security risks caused by the poor management of certificates made by some developers in the Google Play Store.

Certificates (certificate Fingerprint) have been identified as being shared by multiple developers (normally associated with online platforms that facilitate the development of apps). But there are also companies specialising in the development of Android apps that use the same certificate to sign apps associated with several customers.

For the end user, it becomes very difficult to determine if the certificate used to sign the application being downloaded is shared by other applications. This should be a responsibility of the developers or companies that outsource the development of their mobile applications to third parties.

Finally, this study also concludes that a scantly strict management of digital certificates can give way to the mutation of applications. This implies that an application may change developer from one version to another without being guaranteed who is behind its new development. Google does not disclose any information regarding these changes which prevents the user from perceiving the possible risk they incur when downloading an application. This study has shown how the consumption of data sources such as Tacyt facilitates the extraction of a timeline associated with each application or each developer. This example clearly illustrates the consequences of certificate management in Google Play.

[11] http://developer.android.com/guide/topics/manifest/manifest-element.html