Cyberthreats_
Telefónica

Análisis Demográfico de Google Play

07/03/2016

Telefónica

securely powered by
ElevenPaths

Sobre los editores

Cyberthreats_ Telefónica

El objetivo principal del Servicio de Cyberthreats_ de Telefónica es la generación de inteligencia adaptada a las necesidades de nuestros clientes para contrarrestar aquellas amenazas que pudieran derivar del entorno digital. Lo que diferencia a Telefónica de otros servicios tradicionales de seguridad, es la capacidad para tratar de integrar, evaluar y transformar información y datos en bruto en conclusiones y posibles escenarios futuros.

Los tres pilares en los que se apoya el servicio son:

- Detección
- Análisis e interpretación
- Prospectiva y anticipación

ElevenPaths

En ElevenPaths pensamos de forma diferente cuando hablamos de seguridad. Liderados por Chema Alonso, somos un equipo de expertos con inquietud para replantearnos la industria y gran experiencia y conocimiento en el sector de la seguridad. Dedicamos toda nuestra experiencia y esfuerzos en crear productos innovadores para que la vida digital sea más segura para todos.

La evolución de las amenazas de seguridad en la tecnología es cada vez más rápida y constante. Por eso, desde junio de 2013, nos hemos constituido como una start-up dentro de Telefónica para trabajar de forma ágil y dinámica, ser capaces de transformar el concepto de seguridad anticipándonos a los futuros problemas que afecten a nuestra identidad, privacidad y disponibilidad online.

Con sede en España, estamos presentes también en UK, EE.UU, Brasil, Argentina, y Colombia.

Resumen ejecutivo

La cata realizada a principios de febrero de 2016, muestra que Tacyt había diseccionado un total de 3.365.527 aplicaciones de Google Play Store, de las cuales sólo 2.438.864 seguían disponibles para su descarga en el *market*.

Atendiendo a la dirección de correo que utilizan los desarrolladores en Google Play Store (developerEmail), Tacyt dispone de información de 678.328 desarrolladores diferentes. Cerca del 44% de las direcciones de correo presentes en Google Play Store son del dominio "gmail.com".

Google exige a los desarrolladores que firmen todas sus aplicaciones antes de ser publicadas en el Google Play Store. Este certificado se utiliza para identificar al autor de la aplicación. El número total de certificados diferentes encontrados por Tacyt ha sido de 805.731. Aunque la gran mayoría de certificados encontrados están asociados a una única dirección de correo, existen excepciones. Incluso se ha encontrado un certificado relacionado con más de diez mil direcciones de correos diferentes.

La compartición del mismo certificado entre varios desarrolladores no es una práctica recomendable desde el punto de vista de seguridad, puesto que podría llegar a comprometer el proceso de actualización de las apps o la información que estas manejan. De los 805.731 certificados (certificateFingerprint) conocidos por Tacyt, 761.389 están asociados a una sola dirección de correo de desarrollador (developerEmail), el resto es utilizado por dos o más direcciones de correo de desarrollador diferentes para firmar sus aplicaciones. Incluso se ha encontrado un certificado que es utilizado por 10.240 cuentas de correo de desarrollador distintas.

Tabla de contenidos

Introducción

La demografía, del griego *demos* (pueblo) y grafos (trazo), se define como el estudio estadístico de una colectividad humana, referido a un determinado momento o a su evolución[1].

En este sentido, el informe tiene el objetivo de estudiar la población de desarrolladores y aplicaciones en el Google Play Store a principios de febrero de 2016, determinar su dimensión, estructura, evolución y características generales desde un punto de vista cuantitativo.

Como fuente de información se ha utilizado Tacyt, una innovadora herramienta de ciberinteligencia que supervisa, almacena, analiza, correlaciona y clasifica millones de apps móviles mediante su tecnología de big data, añadiendo miles de aplicaciones nuevas cada día[2].

[1] http://dle.rae.es/?id=C9n3LUX
[2] https://www.elevenpaths.com/es/tecnologia/tacyt/index.html

Indicadores demográficos básicos

En Internet existen varias fuentes de información que proporcionan una colección de indicadores básicos con la evolución histórica del número de aplicaciones disponibles en el Google Play Store.

El portal "Statista", especializado en estadísticas, indicaba que en noviembre de 2015 había 1.800.000 apps en el Google Play Store[3]:

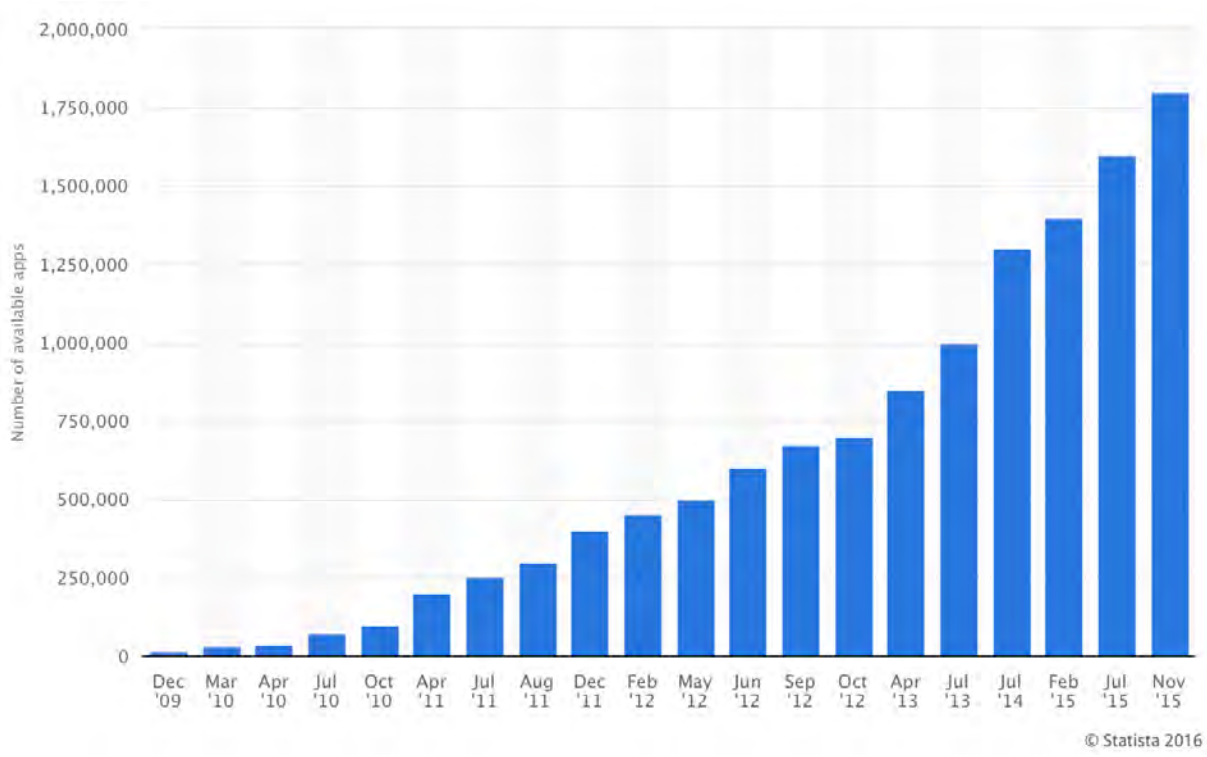

Figura 1. Número apps en Google Play Store (Statista Dic 2009 – Nov 2015)

El directorio de aplicaciones Android, "AppBrain", también ofrece información sobre el número de aplicaciones disponibles en el Google Play Store, además es posible encontrar información adicional como: número mensual de nuevas apps, distribución de valoraciones de las apps, de las descargas, clasificación de apps según su calidad

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

(*low quality vs. regular*), categorías en las que se engloban, aplicaciones más populares, etc. [4]

A principios de febrero de 2016, "AppBrain" indicaba que había cerca de 2 millones de apps disponibles en el Google Play Store.

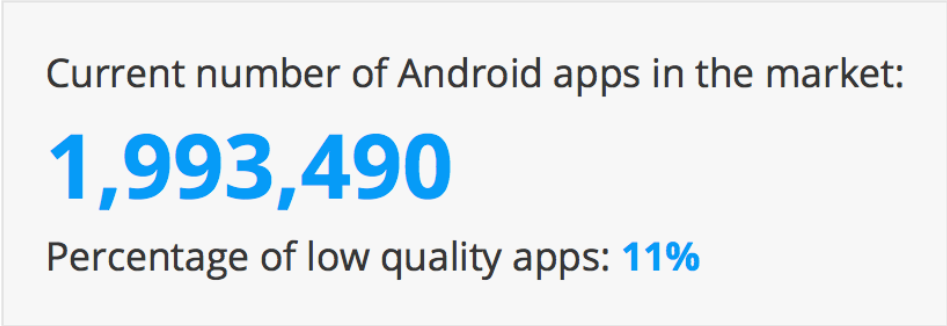

Figura 2. Número apps disponibles en Google Play Store (AppBrain Stats Feb 2016).

Casi medio millón más de las que registraba hace un año:

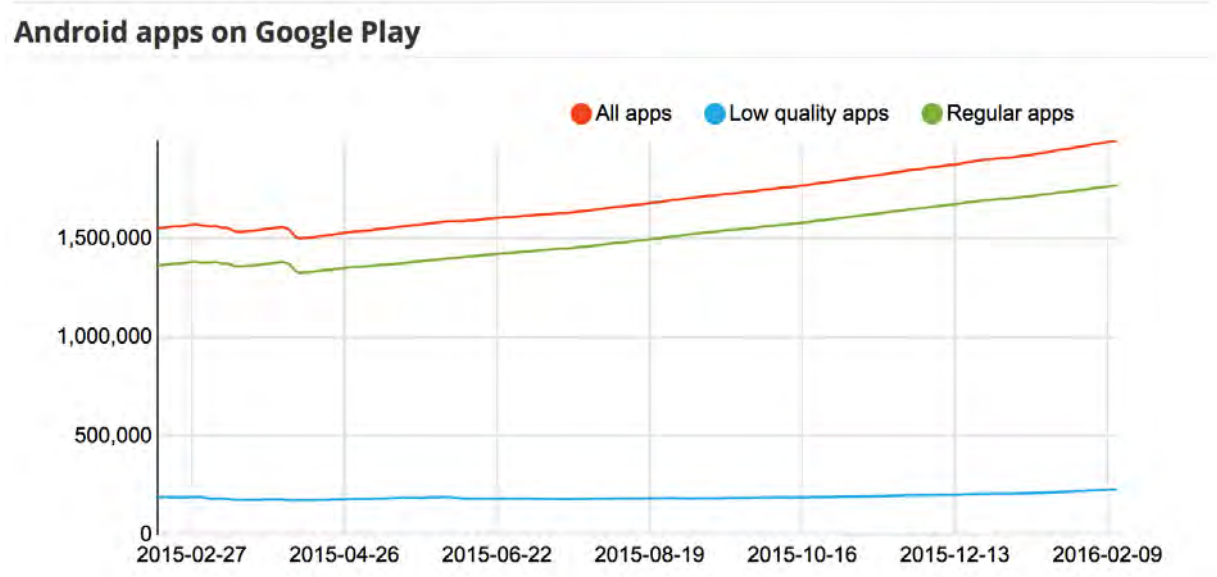

Figura 3. Número apps en Google Play Store (AppBrain Stats Feb 2015 – Feb 2016)

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

Por último, utilizando como fuente "App Annie", a mediados de febrero, el número de apps disponibles se situaba en 2.344.363[5] en Google Play Store:

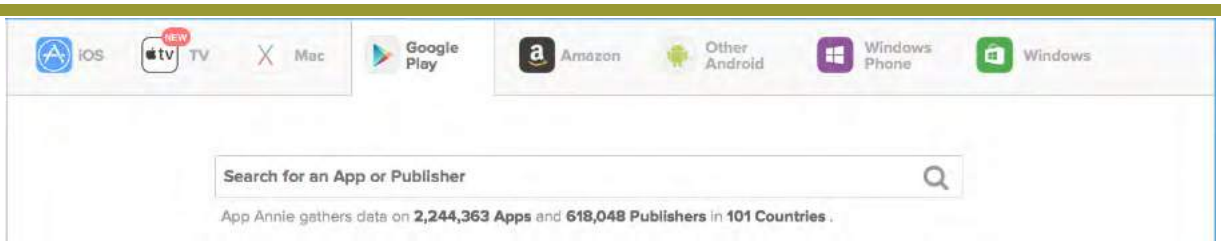

Figura 4. Número apps disponibles en Google Play Store (App Annie Stats Feb 2016).

En esta fuente, a diferencia de AppBrain se ofrece información sobre el número de desarrolladores (*publishers*) y lo sitúa en 618.048 distribuidos en más de 100 países.

Para poder extraer una información más completa relativa a los desarrolladores es necesario acudir a la fuente Tacyt. Analizando la información disponible en Tacyt asociada al Google Play Store obtenemos los siguientes datos:

Tabla I: Información disponible en Tacyt de Google Play Store (Feb 2016)

¿Qué conoce Tacyt de Google Play Store?	Total
Número aplicaciones conocidas por Tacyt	3.365.527
Número aplicaciones distintas (packageName)	2.316.838
Total aplicaciones retiradas (no disponibles ya en Google Play)	926.663
Número de direcciones de correo únicas asociadas a desarrolladores	678.328
Número de nombres de desarrollador distintos	539.468
Número de certificado únicos (certificateFingerprint)	805.731
Número de claves públicas diferentes	805.624

Key Topic: alta tasa de mortalidad de apps

El muestreo realizado a principios de febrero de 2016 muestra que Tacyt guarda un total de 3.365.527 apps de Google Play Store, de las cuales 2.316.838 son aplicaciones distintas (diferente packageName).

Además Tacyt tiene almacenadas cerca de un millón de apps que ya no están disponibles para su descarga en el Google Play Store (bien porque el desarrollador

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

actualizó la versión de su app y eliminó las anteriores, porque decidió retirarla o porque fue Google Play quien la eliminó de su Store).

Key Topic: es difícil determinar el número exacto de desarrolladores únicos

Atendiendo a la dirección de correo que utiliza el desarrollador en Google Play Store (developerEmail), Tacyt dispone de información de 678.328 desarrolladores diferentes. Este orden de magnitud coincide con lo que reportaba App Annie, pudiendo corresponder la desviación entre los números ofrecidos por ambas fuentes a la frescura de la información, que es mayor en el caso de Tacyt.

Figura 5. Detalle información disponible en Tacyt asociada al desarrollador de ejemplo

Centrando el foco en los datos que ofrece Tacyt, es interesante detenerse en la comparación de algunos valores. Por ejemplo, atendiendo al número de nombres de desarrollador diferentes obtenidos (developerName) frente al número de los certificados utilizados para firmar las apps, se pueden plantear varias hipótesis:

- Que un mismo desarrollador pueda estar utilizando varias direcciones de correo.
- Que pueda estar identificándose con varios nombres de desarrollador.
- Que pueda utilizar varios certificados diferentes para firmar las distintas apps que desarrolla

A lo largo de este informe quedará demostrado que esto resulta en una práctica habitual entre los desarrolladores, y que pueden cambiar de nombre, certificado o direcciones de correo habitualmente para intentar disfrazar o diversificar la identidad bajo la que publican. Lamentablemente, con la información que se puede recoger mediante consulta directa a Google Play es imposible reconstruir la línea temporal en la que esta prácticas tienen lugar.

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

Figura 6.Información en Tacyt asociada al certificado con el que se firma la app

Análisis de población

Analizando las 678.328 direcciones de correo asociadas a desarrolladores que Tacyt ha encontrado en el Google Play Store, es sencillo determinar cuáles son los dominios y los *nicknames* más comunes que aparecen en el campo developerEmail (nickname@dominio).

Tabla II: Top 10 dominios utilizados como correo de desarrollador (Febrero 2016)

Developer Email Domain	Nº 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

Tabla III: Top 10 nicknames utilizados como correo de desarrollador (Febrero 2016)

Developer Email nickname	Nº Emails
info	66.430
support	35.141
contact	12.301
android	6.873
apps	6.103
contato	4.178
app	3.076
sales	2.826
webmaster	2.798
hello	2.654

Cerca del 44% de las direcciones de correo presentes en Google Play Store pertenecen al dominio "gmail.com". En total existen más de 286.000 dominios diferentes presentes en los developerEmail. Los más habituales se corresponden con proveedores de correo gratuitos.

En cuanto a los *nicknames*, los más habituales son nombres genéricos de soporte, información o contacto. Dentro del top 10 destaca la palabra "contato" en portugués/brasileiro. El resto suelen tratarse de términos en inglés.

Atendiendo a los TLDs asociados a los dominios encontrados en las direcciones de correo, existen más de 480 TLDs diferentes, casi el 60% de los developerEmail utilizan una dirección de correo ".com":

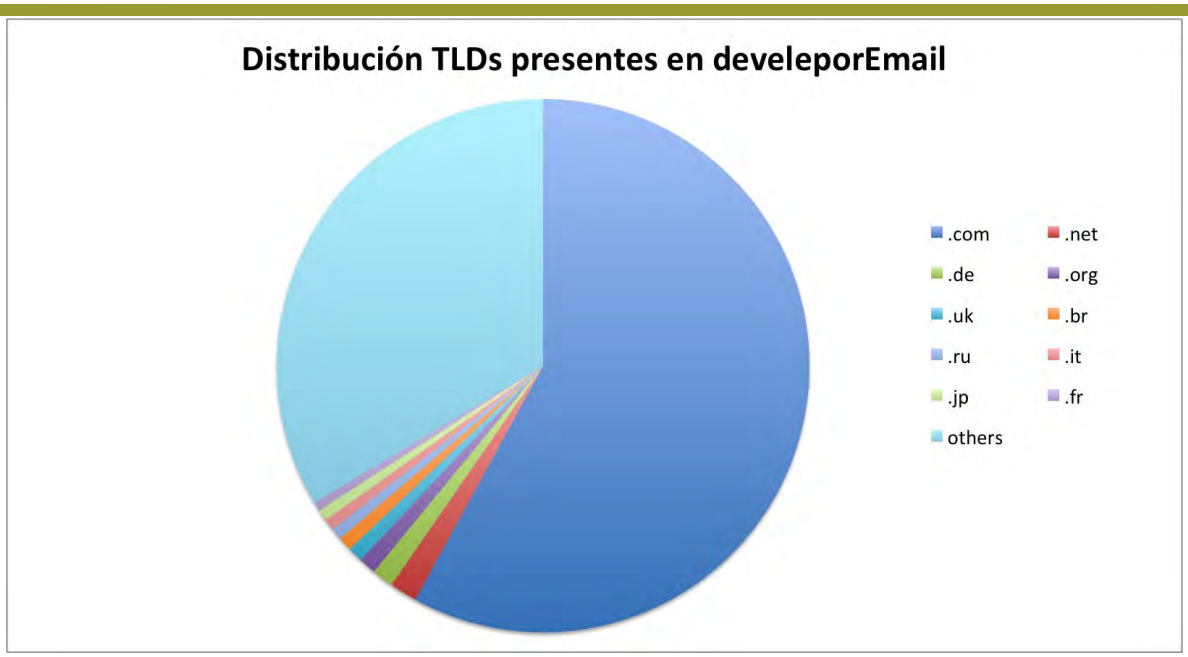

Figura 7. Distribución TLDs encontrados en las direcciones de correo (developerEmail)

Con respecto al TLD ".es" se muestran a continuación los dominios más utilizados, así como los *nicknames* más comunes.

Tabla IV: Top 10 dominios ".es" utilizados como correo de desarrollador (Febrero 2016)

Developer Email Domain	Nº 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

Tabla V: Top 10 nicknames utiliados como correo de desarrollador (Febrero 2016)

Developer Email nickname	Nº Emails
info	1.012
contacto	101
soporte	95
apps	46
android	46
support	42
app	36
admin	36
hola	34
comercial	27

Existen 2.941 dominios ".es" diferentes utilizados por 3.657 direcciones de correo ".es" de desarrolladores distintas.

La siguiente tabla muestra los nombres de desarrollador (developerName) encontrados más comunes, atendiendo al número de apps subidas. Los tres primeros son nombres chinos (en la tabla se incluye su traducción utilizando Google Translate):

Tabla VI: Top 10 nombres de desarrollador con más aplicaciones en Google Play (Febrero 2016)

Developer Name	Nº 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

Del mismo modo se puede obtener también el ranking de correo de desarrollador (developerEmail) en Google Play Store, atendiendo al número total de apps subidas (tanto las que se encuentran actualmente disponibles, como las que no).

Tabla VII: Top 10 direcciones de correo con más aplicaciones subida a Google Play (Febrero 2016)

developerEmail	Nº 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
themesonlyex@gmail.com	2.112
support@reverbnation.com	1.896

En el top ten se encuentran direcciones de correo asociadas a empresas que se dedican al desarrollo software: "Tobit.Software", "CrowdCompass" y "The Church App" entre otras.

Centrémonos ahora en los nombres de desarrollador (developerName) con los que están relacionadas las cuentas de correo más usadas.

La dirección de correo "customer.services@tobil.com" está asociada a 1.385 nombres de desarrollador distintos. La mayoría suelen contener explícitamente la cadena asociada al nombre de la empresa "Tobit.Software". Pero si descartamos los nombres de desarrollador en los que aparezca "Tobit.Software", encontramos un completo listado de otras empresas y sociedades limitadas (GmbH) que han confiado el desarrollo de su aplicación móvil a "Tobit.Software". En las siguientes tablas aparece el detalle de la información encontrada:

Tabla VIII: Top 10 "developerName" asociados a la dirección de correo "customer.services@tobit.com"

Nombre desarrollador	Nº 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

Tabla IX: "developerName" más comunes asociados a "customer.services@tobit.com" en los que no aparece la cadena "Tobit.Software"

Nombre desarrollador	Nº 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

La dirección de correo "drsupport@nobexinc.com" emplea únicamente dos nombres de desarrollador distintos, ambos relacionados con apps móviles para la sintonización de estaciones de radio.

Tabla X: Nombres de desarrollador detrás del correo "drsupport@nobexinc.com"

Nombre desarrollador utilizado	Nº apps
Nobex Technologies	4.314
Rumsey Retro Radio AM 1580	1

Para "support@crowdcompass.com" encontramos 11 nombres de desarrollador diferentes

Tabla XI: Nombres de desarrollador detrás del correo "support@crowdcompass.com"

Nombre desarrollador utilizado	Nº 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

En el caso de "sorokin9910071559@gmail.com" se emplean tan sólo dos nombres de desarrollador distintos.

Tabla XII: Nombres de desarrollador detrás del correo "sorokin9910071559@gmail.com"

Nombre desarrollador utilizado	Nº apps
Andrey Sorokin	2.148
iniCall.com	1.005

Por último, para "help@pocketmags.com" volvemos a encontrar de nuevo once nombre de desarrollador diferentes.

Tabla XIII: Nombres de desarrollador detrás del correo "help@pocketmags.com"

Nombre desarrollador utilizado	Nº 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: las direcciones de correo empleadas en Google Play Store no tienen por qué ser nominativas

Detrás de un determinado developerEmail pueden encontrarse uno o más individuos, o empresas de desarrollo software que utilizan un mismo correo para subir al Google Play Store una serie de apps que pueden estar asociadas a servicios de múltiples y diversas empresas.

Analizando los diferentes nombres de desarrollador es posible determinar la cartera de clientes de empresas que se dedican al desarrollo de apps. En el caso de que un atacante encontrase una vulnerabilidad en una de estas aplicaciones, podría listar fácilmente el conjunto de aplicaciones desarrolladas por el mismo equipo y analizar si son vulnerables también o no.

Esto ya ha ocurrido en el pasado, por ejemplo con AppsGeyser, un creador de aplicaciones "a golpe de clic" que desactivaba la comprobación de certificados SSL en sus aplicaciones. Un atacante en la misma red local que un usuario que utilice estas aplicaciones, podrá inyectar cualquier página cuando navega desde las apps afectadas, o bien ver y modificar webs que deberían estar protegidas[6].

[6] http://blog.elevenpaths.com/2014/12/5500-apps-potencialmente-vulnerables.html

Volviendo al top de direcciones de correo asociadas a desarrolladores que más apps han subido al Google Play Store, podemos examinar el número de apps únicas.

En la siguiente tabla se observa cómo mientras algunos desarrolladores, por ejemplo "support@reverbnation.com", rara vez actualizan las apps que suben al Google Play Store, otros como "help@pocketmags.com" o "themesonlyex@gmail.com" han actualizado una media de tres veces cada app subida.

Tabla XIV: Comparativa apps subidas a Google Play vs apps únicas para el top 10 direcciones de correo con más aplicaciones en Google Play (Febrero 2016)

developer Email	Nº apps	Nº apps únicas
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

También es posible mostrar información sobre las aplicaciones (packageName) que más actualizaciones han tenido desde 2014:

Tabla XV: Top 10 apps con más versiones (Febrero 2016)

Package name	Nº versiones
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 ha detectado 81 actualizaciones para la aplicación "Tweetings for Twitter", lo que supone una media de más de cuatro actualizaciones mensuales.

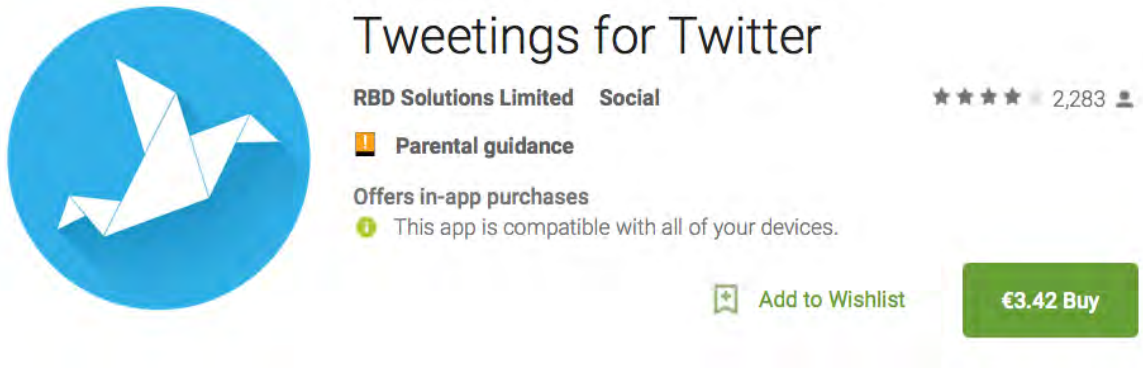

Figura 8. Detalle de la app "Tweetings for Twitter" en el Google Play Store

Atendiendo al número de apps únicas en el Google Play Store, el top 10 de developerEmail sería el que muestra la siguiente tabla:

Tabla XVI: Top 10 direcciones de correo con más aplicaciones subida a Google Play (Febrero 2016)

developer Email	Nº 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

También es interesante analizar cuántos nombres de desarrollador (developerName) diferentes hay detrás de cada correo de desarrollador (developerEmail). En la siguiente tabla se muestran las direcciones de correo que utilizan un mayor número de nombres de desarrollador diferentes:

Tabla XVII: Top 10 developerEmail que utilizan más nombres de desarrollador diferentes (Febrero 2016)

Developer Email	Nº 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

Haciendo el mismo análisis para los correos de desarrolladores que utilizan el TLD ".es":

Tabla XVIII: Top 10 developerEmail (.es) que utilizan más nombres de desarrollador diferentes (Febrero 2016)

developerEmail	Nº 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

Se muestra a continuación los nombres de desarrollador utilizados por las dos direcciones de correo que encabean la tabla anterior:

Tabla XIX: Nombres de desarrollador detrás del correo "info@pressmatic.es"

Nombre desarrollador utilizado	Nº apps
Centro hospitalario Chuac	1
CIRUBUCA	1
Editorial 5150	1
Infolibre	1
itbook	1
Mikel Areitioaurtena	1
PressMatic	1

Tabla XX: Nombres de desarrollador detrás del correo "apps@valenapps.es"

Nombre desarrollador utilizado	Nº apps
Apps Divertidas	1
Colorea Valencia	1
Frases en Español	1
Funny Smartphone Kids	1
Kid Games	1
Messages Apps	1

Análisis de certificados

Google exige a los desarrolladores que firmen todas sus aplicaciones antes de ser publicadas en el Google Play Store. Este certificado es utilizado para identificar al autor de la aplicación. Según la documentación oficial de Google[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.*

Los certificados no tienen que ser generados por una autoridad de certificación, por lo que pueden ser autofirmados. Google indica que la validez del certificado debería ser de al menos 25 años, ya que es imprescindible su utilización en el proceso de actualización de apps. Es responsabilidad del desarrollador mantener la seguridad de la clave privada.

Como se mencionó al principio de este documento,Tacyt es capaz de diseccionar la información asociada al certificado con el que el desarrollador firma cada app del Google Play Store, extrayendo las entidades que se mostraba en la Figura 6.

El número total de claves públicas encontradas en el Google Play Store son 805.624, con ellas se generan un total de 805.731 certificados diferentes (cada uno de estos certificados tiene un certificateFingerprint único).

Sólo se han encontrado tres claves públicas que son utilizadas para generar más de un certificado (certificateFingerprint):

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

Tabla XXI: Claves públicas (primeros caracteres del certificatePublicKey) que generan múltiples certificados

Clave Pública	Nº certificados diferentes
03818d00308189028181009 6f729949a260c7d02275ac68c93b53cbad4cb53...	101
0382010f003082010a028201010090b0b1ebbe3aa1bf4673aef5d8ee09139e...	7
03818d0030818902818100ad04a06c0815469c380d62afd6babe78720c5cdc...	2

Este comportamiento en sí constituye una singularidad en el comportamiento habitual de los usuarios del sistema. Una singularidad no es más que una característica o detalle que distingue un elemento de otros de la misma clase. La importancia de estas singularidades está en el hecho empírico de que normalmente constituyen indicios que conviene investigar.

Key Topic: las singularidades constituyen indicios para llevar a cabo investigaciones

Se muestra a continuación el top 10 tanto de claves públicas atendiendo al número de apps subidas al Google Play Store y firmadas con ellas.

Tabla XXII: Top 10 certificatePublicKey (Febrero 2016)

Clave pública utilizado en el certificado	Nº apps
03818d0030818902818100d6198c6f4685cfcd4435c0efe9f0...	52.129
0382010f003082010a02820101009bbc9e38e883c581fc67dc...	32.988
03818d0030818902818100938cd7ea321af0ef3272fd25d37a...	26.262
0382010f003082010a02820101009ff1622bc9ffc064949cdc...	16.865
03818d0030818902818100b5002784be33acb7a2c03af22989...	13.467
0382010f003082010a0282010100d818a34292de48821d38e7...	9.548
03818d0030818902818100940e7dcb09f198ef35ecae158418...	8.877
0382010f003082010a0282010100dbed9654b7fc556340c1ad...	7.392
03818d0030818902818100 8642b807daef2f28b8ef6badf474...	6.871
03818d0030818902818100a46d9cb660fc2abb60d6459c0e76...	5.255

Existe un relación biunívoca entre las claves públicas y los certificados de las dos tablas anteriores (cada clave pública de la tabla anterior es utilizada para generar

uno y sólo un certificado, cuya huella se corresponde con la que aparece en la misma posición de la tabla que se muestra a continuación).

Tabla XXIII: Top 10 certificateFingerprint (Febrero 2016)

Huella del certificado (certificateFingerprint)	Nº 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

Una buena práctica sería que cada desarrollador generase un certificado único para cada app que publicase en el Google Play Store. Pero viendo las tablas anteriores parece que esto no es así (hay muchas más apps que certificados).

Los certificados son un componente crítico de la seguridad de las aplicaciones que se suben al 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.*

La siguiente imagen muestra la distribución de certificateFingerprint en función del número de apps que firman:

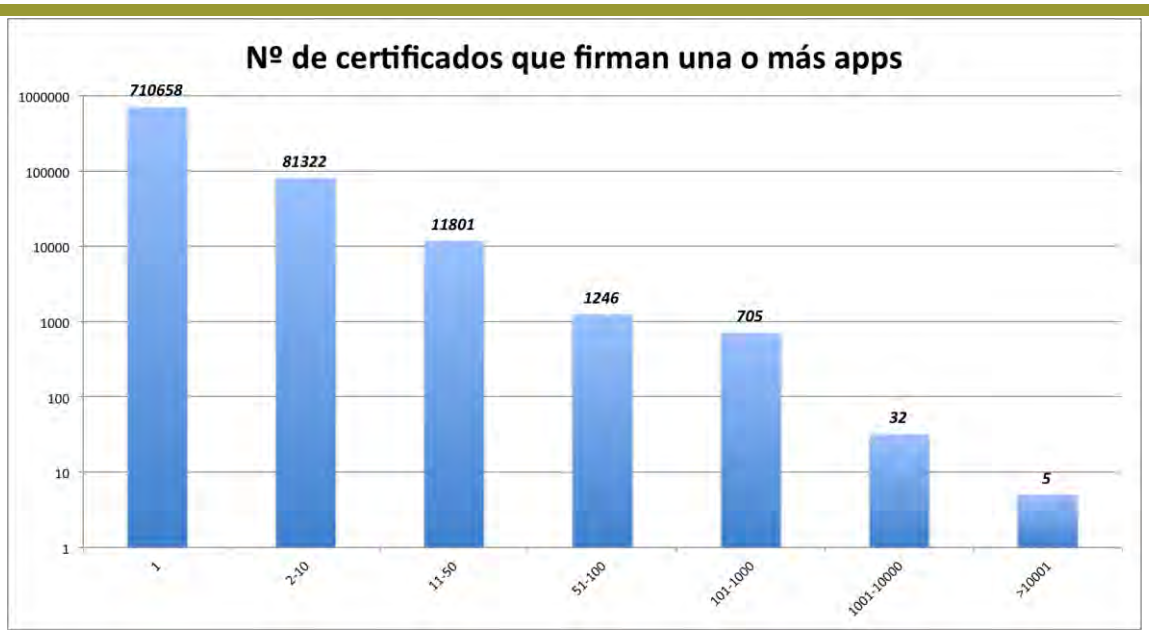

Figura 9. Utilización de certificados para firmar una o más apps

En la figura anterior en el eje X se encuenta el número de aplicaciones que comparten un mismo certificado. El eje Y es el número de certificados que cumplen esta condición.

De los 2.316.838 de apps únicas analizadas, tan sólo 710.658 son firmadas por un certificado que no es utilizado para firmar ninguna otra aplicación.

Existen cinco **certificateFingerprint** que se utilizan para firmar, cada uno de ellos, más de 10.000 apps diferentes,

Es fácil encontrar las empresas que están detrás de estos certificados, la mayoría proporcionan servicios de desarrollo de apps móviles:

Tabla XXIV: Top 10 certificateFingerprint - Empresa relacionada

Huella del certificado (certificateFingerprint)	URL empresa
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

Otra aproximación interesante es conocer si un mismo certificado puede estar siendo compartido por varios desarrolladores. En la siguiente imagen se muestra la distribución de certificateFingerprint en función del número de correos de desarrollador distintos (developerEmail) que lo utilizan para firmar sus apps:

Figura 10. Compartición de certificados entre desarrolladores (developerEmail)

Aunque la gran mayoría de certificados encontrados están asociados a una única dirección de correo, existen excepciones. Incluso se ha encontrado un certificado relacionado con más de diez mil direcciones de correos diferentes.

En la siguiente tabla se muestra el top 10 de certificados (certificateFingenprint) que están siendo utilizados por mayor número de developerEmail.

Tabla XXV: Top 10 certificateFingerprint asociados a mas de un correo (Febrero 2016)

Fingerprint	emais
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: es una mala práctica firmar apps asociadas a clientes o servicios diferentes con el mismo certificado

Aunque una empresa externalice el desarrollo de sus apps móviles es recomendable controlar el certificado con el que se firma la aplicación y gestionar la subida de la app al Google Play Store. Como mínimo debería exigir que el certificado utilizado para firmar su aplicación no sea compartido con terceros, con los que quizás, la empresa no esté interesada en que se la relacione, o en el peor de los casos que puedan acceder a la información que esta maneja.

Podemos analizar también cuántos certificados están asociados a cada una de las direcciones encontradas en el Google Play Store.

En siguiente figura en el eje X se encuentran el número de certificados que están relacionados con una dirección de correo determinada (developerEmail). El eje Y es el número de direcciones de correo que cumplen esta condición.

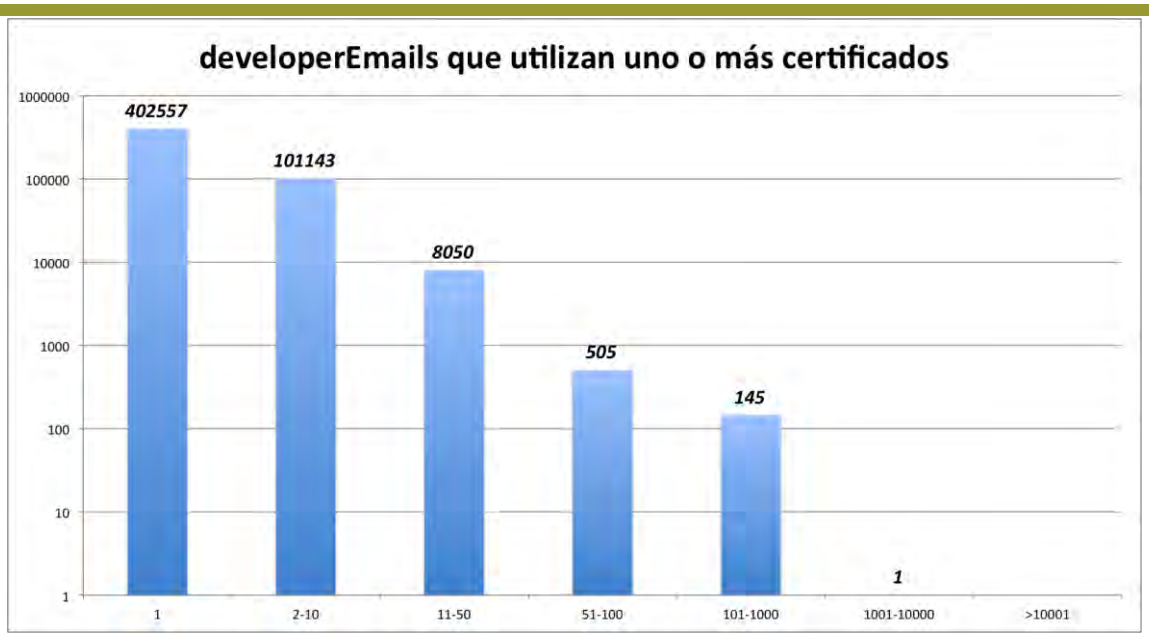

Figura 11. Compartición de certificados entre desarrolladores (developerEmail)

De las 678.328 direcciones de correo conocidas del Google Play Store, más de las tres cuartas partes están relacionadas con un único certificado. No obstante, también existen singularidades como una dirección de correo (developerEmail) que utiliza más de mil certificados para firmar las distintas apps que sube al Google Play Store.

El top 10 de developerEmail que más certificados ha utilizado se muestra a continuación:

Tabla XXVI: Top 10 email con más certificateFingerprint (Febrero 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 permite realizar todo tipo de estadísticas con la información que disecciona de cada uno de los certificados, por ejemplo se muestra a continuación el top 10 de los nombre utilizados por el usuario (Issuer Common Name) para generar el certificado se muestran a continuación:

Tabla XXVII: Top 10 nombre común del usuario que aparece en el certificado (Febrero 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

Analizando por último la validez de los certificados encontrados, como hemos comentado anteriormente Google recomienda un periodo de validez no inferior a 25 años[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.*

En la siguiente imagen se ve la distribución de los periodos de validez encontrados en los certificados analizados.

Un número significativo de certificados no cumple la recomendación/exigencia de Google, teniendo un periodo de validez inferior a 25 años. Incluso se han encontrado 140 certiticados con una validez de 1 año.

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

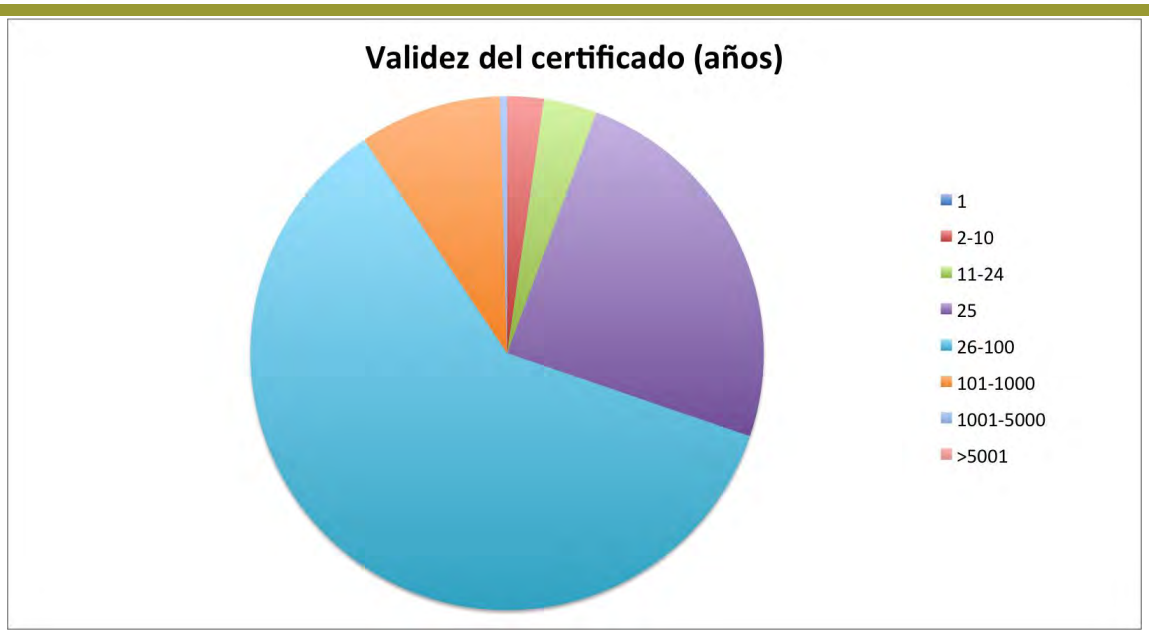

Figura 12. Compartición de certificados entre desarrolladores (developerEmail)

La siguiente tabla muestra el top 10 de tiempos de vida más habituales encontrados en los certificados diseccionados por Tacyt:

Tabla XXVIII: Top 10 duración certificados más comunes (Febrero 2016)

Validez (años)	Nº certificados
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

Ejemplos de interrelaciones entre la población

Se muestran a continuación una serie de gráficas en las que se muestra cómo es posible establecer relaciones entre diferentes ciberidentidades de Google Play Store, ya que comparten determinados recursos (singularidades).

Si analizamos la información disponible en Tacyt de la aplicación "Warframe Mobile Codex" [10]:

Figura 13. Detalle de la app en Google Play Store

Obtenemos el siguiente grafo de relaciones:

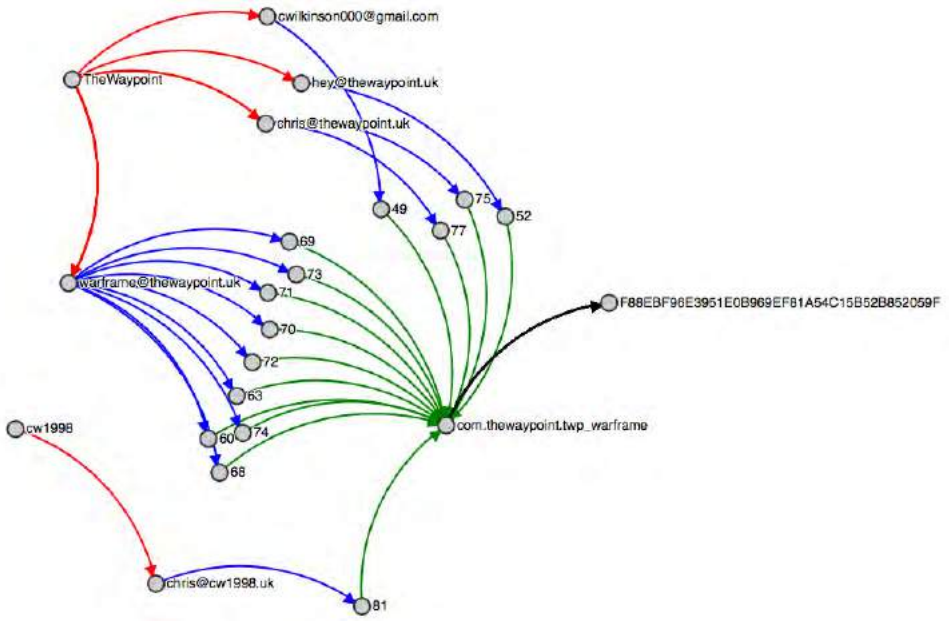

Figura 14. Grafo de relaciones entre ciberidentidades obtenido con Tacyt

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

Tacyt ha descargado de Google Play Store 14 versiones diferentes de esta aplicación, el código de cada versión (versionCode) aparece en la imagen anterior junto a las bolas a las que llegan flechas azules y desde las que salen flechas verdes.

El nombre de la app en Google Play Store (packageName) es "com.thewaypoint.twp_warframe" y está representada en la imagen anterior por la bola a la que llegan las fechas verdes y de la que sale una única flecha negra hacia la entidad asociada al certificado con el que se firma la app (certificateFingerprint). Todas las versiones han sido firmadas con el mismo certificado.

No obstante, si analizamos la parte izquierda de la figura, podemos observar como a lo largo del tiempo el nombre del desarrollador (developerName: bolas desde las que salen las flechas rojas) y las direcciones de correo asociadas al mismo (developerEmail: bolas a las que llegan las flechas rojas y de las que salen flechas azules) han ido cambiando a lo largo del tiempo según se iban publicando nuevas versiones de la aplicación:

- El nombre de desarrollador que utilizaba en las 13 primeras versiones era "TheWayPoint" y llegó a utilizar hasta cuatro correos diferentes. Inicialmente un correo de Gmail y posteriormente tres cuentas distintas asociadas al dominio "thewaypoint.uk".
- En la última versión disponible, el nombre de desarrollador ha cambiado a "cw1998" y el correo asociado al desarrollador ha pasado a ser "chris@cw1998.uk".

Otro tipo de relaciones que pueden obtenerse fácilmente es a partir de la compartición de certificados (certificateFingerprint) con la que varios desarrolladores firman sus apps.

En la siguiente figura los nombres de los desarrolladores (developerName) son el origen de las fechas rojas que terminan en las direcciones de correo (developerEMail) utilizadas por el desarrollador y desde estas salen fechas azules apuntando a la huella del certificado (certificateFingerprint) que han empleado para firmar las apps que han subido al Google Play Store.

Figura 15. Relaciones entre ciberidentidades por utilizar los mismos certificados

Por último, también es posible representar relaciones débiles entre ciberidentidades utilizando singularidades como el periodo de validez con el que se ha generado el certificado (en el caso que se muestra a continuación 2.873 años):

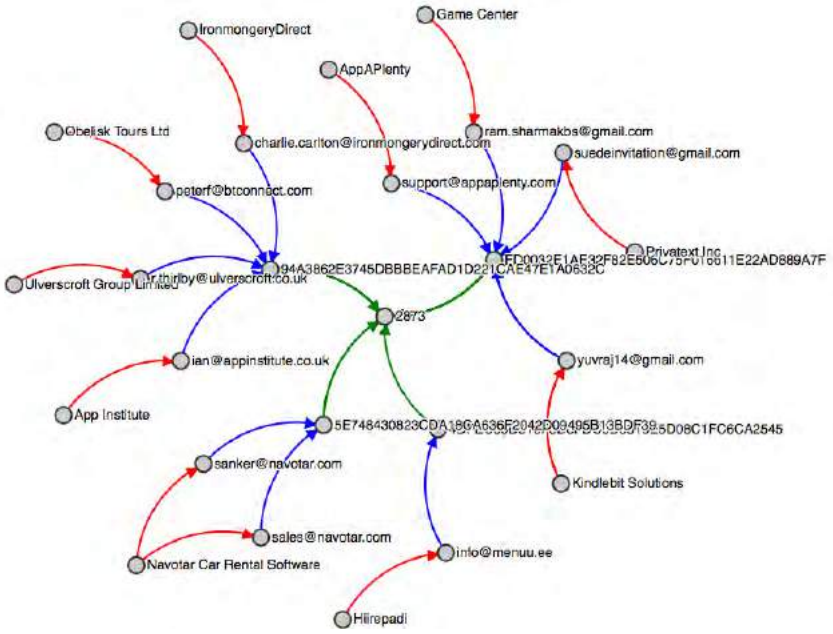

Figura 16. Relaciones débiles entre ciberidentidades a partir de una singularidad como el periodo de validez del certificado utilizado para firmas las apps

En la figura anterior los nombres de los desarrolladores (developerName) son el origen de las fechas rojas que terminan en las direcciones de correo (developerEMail) utilizadas por el desarrollador. Desde estas direcciones salen fechas azules apuntando a la huella del certificado (certificateFingerprint) que han utilizado para firmar las apps que ha subido al Google Play Store. Finalmente desde cada certificateFingerprint sale una flecha verde hacia la entidad asociada al periodo de validez del certificado, en este caso 2873 años.

Conclusiones

La primera conclusión que se puede extraer de este informe es la altísima variabilidad del mercado de aplicaciones de Google Play. Revisando los números a lo largo de los meses que lleva en marcha Tacyt se puede afirmar que el promedio diario de nuevas aplicaciones es de 4.500 y se ha mantenido con escasa variación.

En este análisis se ha verificado cuál es la tendencia en término de procedencia de los desarrolladores y características asociadas a las alternativas que usan para identificarse en el sistema. Al margen del interés estadístico que posée la información mostrada en la primera parte del documento (información de los TLD más presentes o nombres de usuario), se pretende remarcar qué impacto tienen estas alternativas cuando se las relaciona con el uso de certificados digitales, en la precisión de la identificación de los desarrolladores. De hecho un posible hecho que puede explicar en parte las causas de este rápido y continuado crecimiento es la política laxa en la identificación de los desarrolladores de apps que ha mantenido Google Play desde su origen. Aunque el uso de certificados digitales para la firma de software debería identificar de forma univoca al individuo o la entidad que está detrás del propio software, este informe muestra con números que Google Play facilita el abuso de este concepto y esto puede dar lugar a situaciones en las que dicha identificación quede comprometida.

Cuando un desarrollador (developerEmail) firma su aplicación Android (packageName), con un determinado certificado (certificateFingerprint) y la sube al Google Play Store, ya no hay vuelta atrás. Ni esa aplicación, ni sus actualizaciones podrán ser firmadas con un certificado diferente dentro del ecosistema de Google.

Los certificados son un componente crítico de la seguridad de las aplicaciones que se suben al Google Play Store. Si un desarrollador desea utilizar un certificado diferente para firmar la actualización de una de sus aplicaciones (por ejemplo, porque haya perdido el certificado utilizado inicialmente), deberá retirar la aplicación original y publicar la actualización como si se tratase de una aplicación nueva (con un packageName diferente).

La huella de certificado (certificateFingerprint) utilizada para firmar una aplicación, además de fijar quién podrá realizar una actualización de la misma, también establece una relación de confianza con aquellas aplicaciones que han sido firmadas con el mismo certificado, fijando con que otras puede compartir datos durante su ejecución.

Android permite a las aplicaciones firmadas con el mismo certificado ejecutarse en el mismo proceso (siempre que compartan también *sharedUserID*[11]), logrando así que el sistema las trate como una sola aplicación (compuesta por varios módulos). Además posibilita la compartición de datos y funcionalidades de manera segura entre aplicaciones (la comprobación de permisos está basada en el certificado con el que se firman las aplicaciones)

A partir del análisis realizado, se pueden identificar varios riesgos de seguridad causados por la mala gestión de certificados que realizan algunos desarrolladores en el Google Play Store.

Se han identificado certificados (certificateFingerprint) que son compartidos por múltiples desarrolladores (normalmente asociados a plataformas online que facilitan el desarrollo de apps). Pero también existen empresas especializadas en el desarrollo de apps Android, que utilizan el mismo certificado para firmar apps asociadas a varios clientes.

Para el usuario final resulta muy difícil determinar si el certificado con el que se ha firmado la aplicación que se está descargando es compartido por otras aplicaciones, esto debería ser responsabilidad de los desarrolladores o de las empresas que subcontratan el desarrollo de sus aplicaciones móviles a terceros.

Por último, también es una conclusión de este estudio el que una gestión poco estricta de certificados digitales puede llegar a facilitar la mutación de las aplicaciones. Esto supone que una aplicación pueda cambiar de desarrollador de una versión para otra sin que se garantice quién está detrás de su nuevo desarrollo. Google no facilita ninguna información relativa a estos cambios con lo que el usuario no percibe el posible riesgo que asume al descargar una aplicación. En este estudio se ha mostrado cómo el consumo de fuentes de datos como Tacyt facilita la extracción de una línea temporal asociada a cada aplicación o cada desarrollador. Este ejemplo ilustra bien las consecuencias que tiene la gestión de certificados por Google Play.

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