Telefónica | BUSINESS SOLUTIONS   POWERED BY ElevenPaths

Descubre los secretos de la comunidad de Google Play

Una historia sorprendente

basada en el estudio demográfico del mercado de aplicaciones de Google realizado con Tacyt en febrero de 2016

Érase una vez...

...una tienda online donde se distribuían apps para dispositivos móviles con sistema operativo Android y al que llegaban una media de 4.500 nuevas cada día.

Pero todas ellas no eran desarrolladas por sus padres, los desarrolladores, de una forma adecuada a pesar de ser conscientes de que sus archienemigos, los ciberdelincuentes, estuvieran buscando su oportunidad.

Todo continuó así hasta que llegó Tacyt, una herramienta de ciberinteligencia que detectaba quienes no hacían bien su trabajo.

Google Play

Primeros descubrimentos

Tras el duro trabajo de preguntar a cada una de las apps cómo se llamaban, por quiénes habían sido desarrolladas y otros detalles íntimos, Tacyt le revela a Junior, nuestro analista, los siguientes datos:

Número de **APLICACIONES** (packageName)

TOTALES	3.366 K
DISTINTAS	2.317 K
RETIRADAS	927 K

Como ves, existe una alta tasa de mortalidad de las apps.

¿Por qué es tan importante almacenar información sobre apps retiradas del mercado oficial?

En ocasiones, los desarrolladores deciden retirar aplicaciones a las que no seguirán dando soporte pero, en otras, la retirada se debe a prácticas maliciosas que los analistas no podrían investigar de otra manera.

Número de direcciones de **EMAIL** ÚNICAS DE DESARROLADORES (developerEmail): 678 K

Número de nombres de **DESARROLLADOR** DISTINTOS (developerName): 539 K

Número de **CERTIFICADOS** ÚNICOS (certificateFingerprint): 806 K

¡No entiendo!

¿Es que Google Play permite a un mismo desarrollador utilizar direcciones de correo o nombres diferentes, o incluso, varios certificados para firmar distintas aplicaciones?

¡Así es!

Resulta que son prácticas que suelo detectar de forma habitual y, en ocasiones, tienen el objetivo de disfrazar la verdadera identidad de los desarrolladores.

4 relaciones reveladoras

Preste atención a las indicaciones que Tacyt proporciona a Junior para comprender la complejidad de Google Play

1

CERTIFICADOS ÚNICOS (certificateFingerprint): 806 K — **DIRECCIONES DE EMAIL ÚNICAS** (developerEmail): 678 K

De los 805.731 certificados conocidos, 761.389 están asociados con una sola dirección de correo de desarrollador. El resto son utilizados por dos o más direcciones de correo de desarrollador diferentes para firmar sus aplicaciones.

¡He llegado a encontrar un certificado que es utilizado por 10.240 cuentas de correo distintas!

2

NOMBRES DE DESARROLLADOR DISTINTOS (developerName): 539 K — **APLICACIONES TOTALES** (packageName): 3.366 K

Ocurre de igual manera con los nombres de los desarrolladores.

Para que te hagas una idea, el desarrollador que más apps tiene es un tal *Tenchijin Horoscopes* y ha firmado hasta 7.102 apps diferentes.

3

CERTIFICADOS UNICOS (certificateFingerprint): 806 K — **APLICACIONES TOTALES** (packageName): 3.366 K

Otro dato interesante, ¡existen más aplicaciones que certificados!

¿Sabes cuántas apps tiene asociadas el certificado que más apps comparte?

¡52.129!

4

NOMBRES DE DESARROLLADOR DISTINTOS (developerName): 539 K — **DIRECCIONES DE EMAIL UNICAS** (developerEmail): 678 K

Como ves, las direcciones de email pueden no ser nominativas. Detrás de una dirección podemos encontrar apps asociadas a una o más personas o empresas.

La dirección de correo que más apps comparte pertenece a una empresa llamada *Tobit* dedicada al desarrollo de software.

Algunas implicaciones para la seguridad

Debes recomendar a las empresas que, si externalizan el desarrollo de sus aplicaciones, exijan que el certificado no sea compartido.

Así podrían evitar que se les relacione con el resto de la cartera de clientes de la empresa desarrolladora de apps.

CONTROLA TU CERTIFICADO SI NO QUIERES COMPARTIR INFORMACIÓN CON TERCEROS

¿Qué consecuencias tendría que se pudiera listar la cartera de clientes de una empresa desarrolladora?

En el caso de que un atacante encontrase una vulnerabilidad en una de las aplicaciones, se podría enumerar fácilmente el conjunto de apps desarrolladas por el mismo equipo y analizar también si son vulnerables.

ES POSIBLE ENUMERAR APLICACIONES CON LAS MISMAS VULNERABILIDADES

Puedes leer al completo nuestro análisis demográfico de Google Play en nuestro blog: **blog.elevenpaths.com**

No te pierdas ninguno de nuestros informes: **visita elevenpaths.com o síguenos en Twitter @ElevenPaths y LinkedIn**

Telefónica | BUSINESS SOLUTIONS   POWERED BY ElevenPaths