Universidad de Alcalá
Escuela Politécnica Superior

GRADO EN SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

Distribución de malware a través de tiendas de aplicaciones móviles

Autor: Laura Padial González
Tutor/es: José María Gutiérrez Martínez

2017/2018

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

"DISTRIBUCIÓN DE MALWARE A TRAVÉS DE TIENDAS DE APLICACIONES MÓVILES"

Autora: Laura Padial González

Director: José María Gutiérrez Martínez

Tribunal:

Presidente: .....

Vocal 1º: .....

Vocal 2º: .....

Fecha: ..... de ..... de .....

Palabras Clave

Tiendas de aplicaciones móviles, malware, Play Store, aplicación

KeyWords

Mobile application stores, malware, Play Store, application

Resumen corto

Este proyecto trata de un estudio sobre la seguridad de las diferentes tiendas de aplicaciones móviles que nos encontramos hoy en día en nuestros dispositivos, Tienda de Windows Phone, AppStore de iOS y Play Store de Android. Se violará la seguridad de Play Store y se introducirá en la plataforma una aplicación con un malware inofensivo.

Short summary

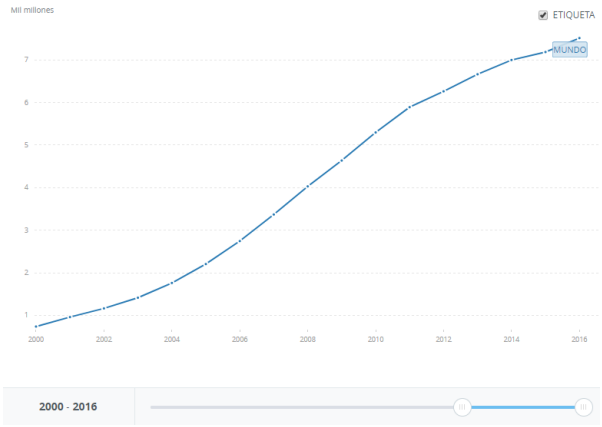
This project is about a study on the security of the different mobile application stores that we find today in our devices, Windows Phone Store, iOS App Store and Android Play Store. The security of the Play Store will be violated and an application with a harmless malware will be introduced on the platform.

Índice resumido

Índice detallado

1. Introducción

Actualmente el número de líneas de telefonía móvil supera la población en el mundo, la cual es de aproximadamente 7400 millones de personas, esta cifra es menor que la del número de líneas móviles la cual alcanza los 7900 millones, y se espera que incremente como podemos observar que ha hecho, año tras año, en la siguiente gráfica.

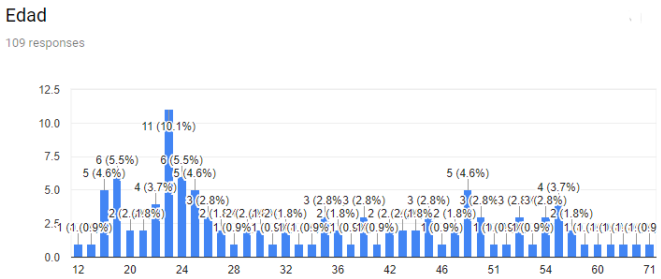


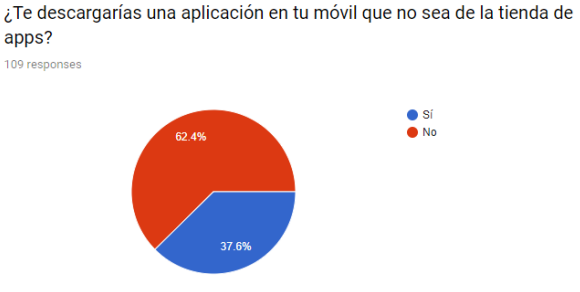
Debido a que aproximadamente el 90% de la población dispone de un teléfono móvil se realizan más accesos a Internet desde estos dispositivos que desde ordenadores por lo que son una plataforma codiciada por los hackers para realizar sus actividades delictivas, como el robo de información, credenciales, ficheros, phishing, etc.

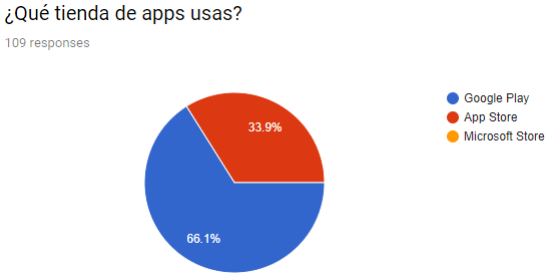
Este documento se trata de una investigación sobre malwares en apps que podemos descargar desde tiendas de aplicaciones móviles y un intento de inserción de una aplicación maliciosa en Google Play, para mí tiene suma importancia debido a que, dada mi experiencia en el trato con el usuario, me han demostrado que tienen más confianza de la que se debe en las tiendas de aplicaciones móviles, he tratado con personas que piensan que solo se pueden infectar con malwares en ordenadores, o que dispositivos con sistema operativo iOs están totalmente protegidos.

He realizado una encuesta, en mayo de 2018 en Google Docs para demostrarlo, ya que no he encontrado ninguna estadística en Internet, donde se puede comprobar la ignorancia que tiene la población con respecto al tema que vamos a tratar la distribución de malwares en tiendas de aplicaciones móviles, y mis resultados han sido los esperados.

https://docs.google.com/forms/d/e/1FAIpQLSdH_fHZESJaLdDrodceTIKOIVBdtodiMUHRtft2UAsjJGn_Fg/viewform







La encuesta se les realizó a 109 personas de todas las edades, y un poco más de la mitad piensan que no es posible que sus dispositivos sean infectados al descargar una app de la tienda de aplicaciones móviles que usan, la mayoría piensan que las empresas revisan todas las apps con el objetivo de que no puedan contener virus, pero una pequeña parte que les siguen piensan que los dispositivos móviles no pueden contener virus.

Debido a que existen personas que desconocen su vulnerabilidad frente a estos ataques y la seguridad que están poniendo hoy en día en las empresas me encuentro muy interesada en la investigación sobre los malwares en las tiendas de aplicaciones móviles, por la posterior divulgación de información a las personas para que piensen si las aplicaciones que van a descargar son de fuentes fiables, son necesarias para ellos o se las descargan meramente por probarlas, pudiendo satisfacer el gusto de otros al infectarlos.

En los siguientes apartados de este proyecto se contemplarán los objetivos que se abarcarán en el desarrollo del proyecto, así como el estado y la evolución de las plataformas más importantes de aplicaciones móviles como son Google Play, App Store y Microsoft Store, y los problemas encontrados en ellas, el desarrollo de la aplicación su funcionalidad y el malware que alberga, el presupuesto necesario para realizar este proyecto y las conclusiones que he obtenido.

Posteriormente, damos paso a comentar el objetivo principal de este trabajo.

2. Objetivo

El objetivo principal de este trabajo de fin de grado consiste en investigar la seguridad en las diferentes tiendas de aplicaciones móviles, principalmente la de Google Play, donde comprobaremos de primera mano la dificultad de introducir una aplicación con código malicioso.

Para cumplir el objetivo realizaremos una serie de pasos:

- Estudiar los malwares más importantes que se han introducido en las actuales tiendas de aplicaciones móviles oficiales instaladas en nuestros dispositivos, Google Play, App Store y Microsoft Store.
  Se explicará en qué tienda de aplicaciones se introdujeron y, se intentará averiguar, qué técnicas se usaron para poder hacerlo, cómo les afectó a los usuarios que se la descargaron y qué beneficios obtuvieron sus desarrolladores, cómo fue su desarrollo, por cuánto tiempo estuvieron disponibles para su descarga y cómo se percató la empresa de su distribución.
  Además, se estudiarán el comportamiento de los diferentes malwares.

- Informarnos sobre las normas y los mecanismos de control que realizan las empresas para la detención de estas aplicaciones infectadas.
  Para ello se estudiarán los acuerdos de política de desarrolladores y el código de conducta de las diferentes tiendas de aplicaciones, explicaremos las consecuencias que se deberán asumir en caso de qué la aplicación que infringe una norma de conducta sea detectada y, además, se realizará una comparación de las normas a seguir para insertar una aplicación en cada una de las tiendas con lo que podremos saber qué empresa es más restrictiva a la hora de permitir albergar aplicaciones en su tienda.

- Crear una aplicación para Android con un malware e introducirla en Play Store, esta aplicación no tendrá efectos nocivos y se tomarán las precauciones debidas para que no se vulnere ninguna ley.
  Para realizar este objetivo debemos tener en cuenta los puntos estudiados anteriormente, se estudiarán los pasos a seguir para alojar una aplicación en Play Store, y el lenguaje de programación Android.
  En el caso de que la aplicación se lograra insertar se avisaría a Google de que se ha insertado correctamente y del malware que contiene, o de lo contrario, nos aseguraríamos de que realmente estamos protegidos de descargarnos una aplicación de Google Play con un malware del tipo insertado.

Con este proyecto se tratará de mostrar la vulnerabilidad que existe hoy en día en las tiendas de aplicaciones móviles en las cuales existe un vector de ataque muy importante para afectar a los usuarios, por lo que las compañías que albergan estas tiendas de

aplicaciones deberían seguir trabajando en mejorar la seguridad y los procedimientos de control de las mismas.

A continuación, damos paso al estado del arte donde se estudiarán los malwares de las apps albergadas en tiendas de aplicaciones móviles, y las normas y mecanismos de control que usan las empresas para la detección de las aplicaciones infectadas.

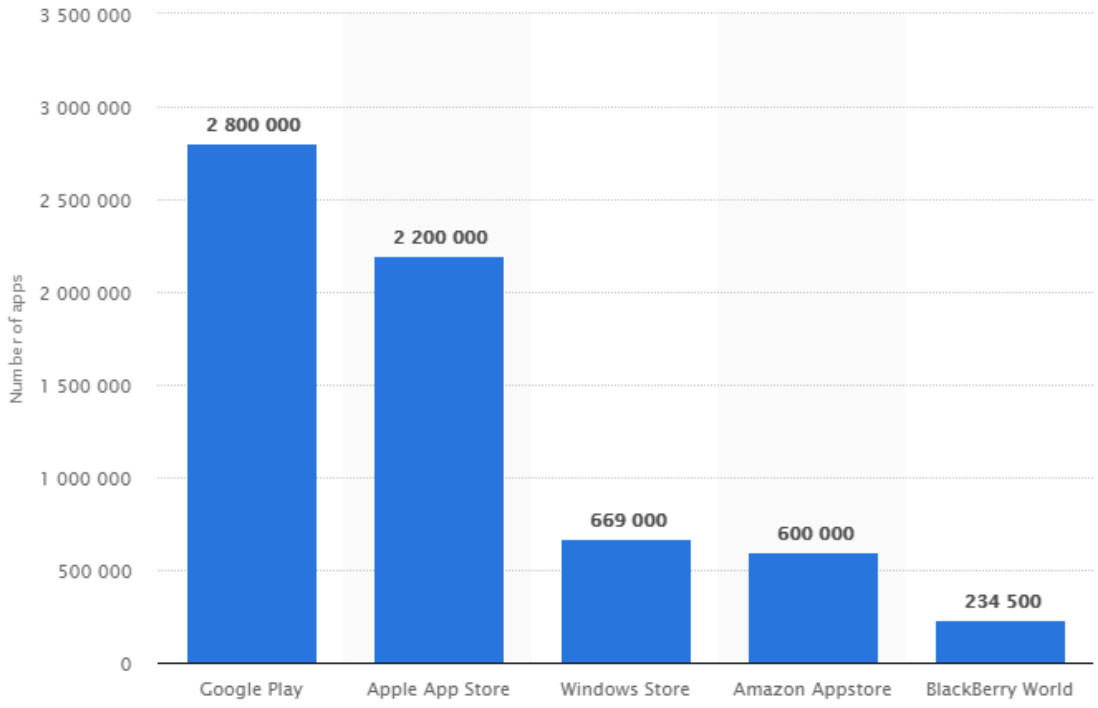
3. Estado del arte

En esta sección se estudiará el negocio actual de las tiendas de aplicaciones móviles, los diferentes tipos de malwares que podemos encontrar en el software, y las normativas de las diferentes empresas a la hora de albergar una aplicación en sus plataformas.

3.1. Tiendas de aplicaciones móviles en la actualidad

En primer lugar, se procede a analizar la situación en la que se encuentran cada una de las tres tiendas de aplicaciones móviles oficiales:

Las tiendas de aplicaciones móviles de Google y Apple están ahora mismo en auge, cada día se albergan en ellas más aplicaciones, sin embargo, nos encontramos un grave problema con la tienda de Microsoft, Microsoft Store, en la cual el número de aplicaciones es bastante reducido.



Número de aplicaciones en las diferentes tiendas a marzo de 2017

Debido a este problema, se explicarán por separado las plataformas App Store y Google Play de la plataforma Microsoft Store que veremos a continuación.

3.1.1. Microsoft Store

Microsoft ha estado adoptando medidas desde sus inicios para albergar más apps en su tienda de aplicaciones móviles y así apaliar la situación de la que hablábamos anteriormente.

En 2012 se lanzó la tienda Windows Phone Store, la cual alcanzó su auge en 2015 con aproximadamente 669000 aplicaciones disponibles, pero eran de mala calidad, por lo que Microsoft fue eliminándolas de su tienda.

Viendo el éxito que gozaba la App Store de Apple, Microsoft lanzó el proyecto Islandwood, el cual consiste en un programa para que los desarrolladores de aplicaciones iOs puedan trasladarlas a Windows 10 Mobile con facilidad, sin modificar demasiadas líneas de código, además estudia la compatibilidad de la aplicación para Windows Phone Store y se ofrecía una guía para desarrolladores desde Redmond. También, han intentado lanzar su símil con Android, llamado el proyecto Astoria, pero finalmente fue cancelado.

En 2015, Microsoft desarrolló la plataforma universal de Windows (UWP) que permite crear aplicaciones compatibles con los diferentes dispositivos de Microsoft, tablets, ordenadores, móviles y la videoconsola Xbox One entre otros, las cuales se distribuyen desde su tienda. Con este proyecto se pretendía incentivar el desarrollo de aplicaciones para Windows Phone Store, además Microsoft alardeaba de la protección que incluía para evitar la copia del software, pero recientemente en febrero de 2018, y aunque esta tecnología no ha tenido mucho éxito, se ha podido vulnerar la protección del primer juego que ha utilizado esta plataforma, Zoo Tycoon Ultimate Animal Collection, saltándose su sistema anticopia, por lo que se espera que Windows refuerce la seguridad de las aplicaciones UWP.

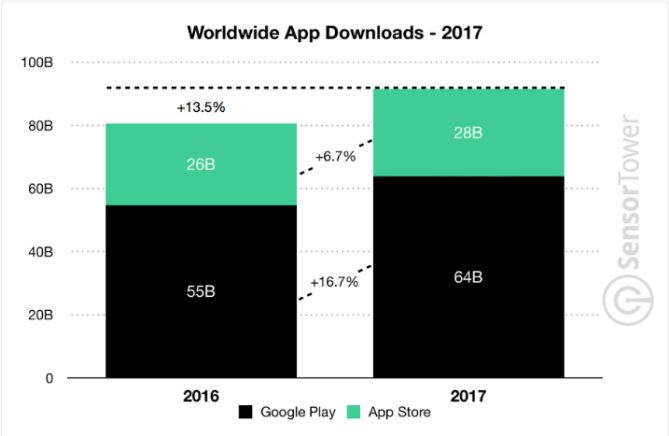
A finales de 2017, Windows Store pasó a llamarse Microsoft Store a raíz de la actualización de Windows 10 “Fall Creators Update”, y también en estas fechas fue anunciada la retirada de la línea de negocio de desarrollo de sistemas operativos para teléfonos móviles, aunque aseguran dar soporte a Windows 10 Mobile durante algún tiempo.

A lo largo del desarrollo de este proyecto estaremos pendientes a la nueva vulnerabilidad encontrada en la tienda de aplicaciones de Microsoft que afecta a las esperanzadoras aplicaciones universales, denominadas apps UWP.

3.1.2. Google Play y App Store

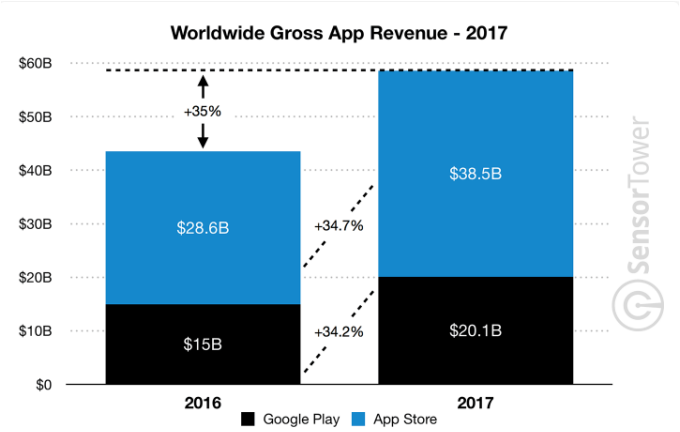
Debido a la diferencia del número de aplicaciones que albergan Google Play y App Store frente a Microsoft Store, procedemos a realizar una comparativa de estas dos grandes tiendas de aplicaciones tanto en el número de descargas de apps como en los beneficios que generan.

Este último año han crecido las descargas de aplicaciones en ambas tiendas, estas descargas se cuentan una sola vez por cuenta de Google o de Apple que se posea, es decir, aunque una persona se compre otro móvil y se descargue una aplicación que tenía en el antiguo, si se trata de la misma cuenta de Google o de Apple, esta aplicación no se contará como descargada nuevamente.



Descargas de aplicaciones

El año pasado se descargaron un 13.5% de aplicaciones más que el anterior, Google Play que cuenta aproximadamente con 600000 aplicaciones más que App Store, ha sido la tienda de aplicaciones líder en descargas, sin embargo, no lo ha sido en rentabilidad, donde Apple ha logrado obtener más del doble de beneficio económico que Google.



Ingresos de las aplicaciones

Esto se podría deber al llamado efecto lujo, los móviles de Apple son de gama alta por lo que las personas que lo adquieren generalmente tienen un poder adquisitivo más alto que las personas que adquieren un móvil Android, de esta misma forma es más probable que los usuarios de Google Play prefieran alternativas gratuitas.

Algunos estudios recomiendan a Android crecer más en las gamas más altas de smartphones para que Google pueda mejorar su estrategia con la cual aumentar los ingresos a través de su tienda de aplicaciones.

Después de estudiar la situación de ambas tiendas de aplicaciones con respecto al mercado, damos paso a ver las vulnerabilidades de seguridad que han presentado Google Play y Play Store respectivamente hasta el año 2018.

Google Play

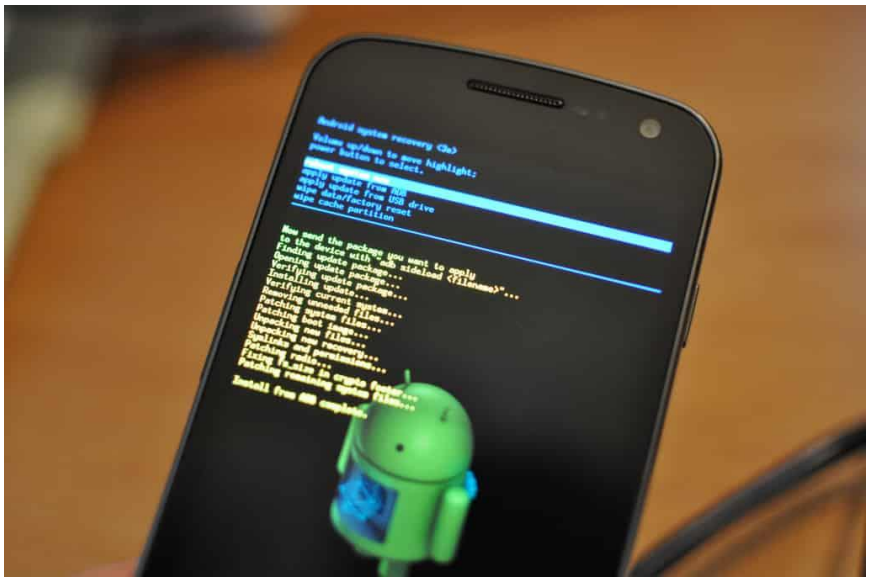
En enero de 2018 Google compartió un comunicado en el cual informaba sobre las aplicaciones y desarrolladores maliciosos con los que se habían topado en 2017.

Se eliminaron más de 700000 aplicaciones que violaban su política, por lo cual ellos han reducido a la mitad las probabilidades de insertar una aplicación maliciosa en su tienda.

El 99% de las aplicaciones con contenido abusivo se eliminaron antes de ser instaladas a través de nuevos modelos y técnicas de aprendizaje automático.

También han sido creados nuevos modelos y técnicas de detención para los desarrolladores que reinciden a crear una app maliciosa, siendo más difícil la creación de nuevas cuentas por estas personas, gracias a ello se eliminaron aproximadamente 100000 cuentas de desarrolladores.

Entre los diferentes tipos de aplicaciones retiradas destacan aquellas en las que se intenta engañar a los usuarios haciéndose pasar por aplicaciones famosas, de las cuales se eliminaron más de 250000 apps el año pasado, las que albergaban contenido inapropiado como puede ser pornografía, violencia, odio o actividades ilegales, de estas se retiraron más de 20000 apps, y las aplicaciones potencialmente dañinas, las cuales contienen un malware que daña los dispositivos o recoge información de las personas sin su consentimiento, Google Play invierte mucho dinero en eliminarlas y ha lanzado Google Play Protect 2017 un antivirus para mantenernos alejados de ellas, además dicen que año tras año se produce un decremento de un 50% de la cantidad de aplicaciones con malware que se insertan en su tienda de apps, aunque saben que todavía algunas aplicaciones podrían evadir sus capas de defensa, con lo que solo pueden continuar mejorando sus capacidades para detectar y proteger a los usuarios contra las aplicaciones maliciosas y sus desarrolladores.



App Store

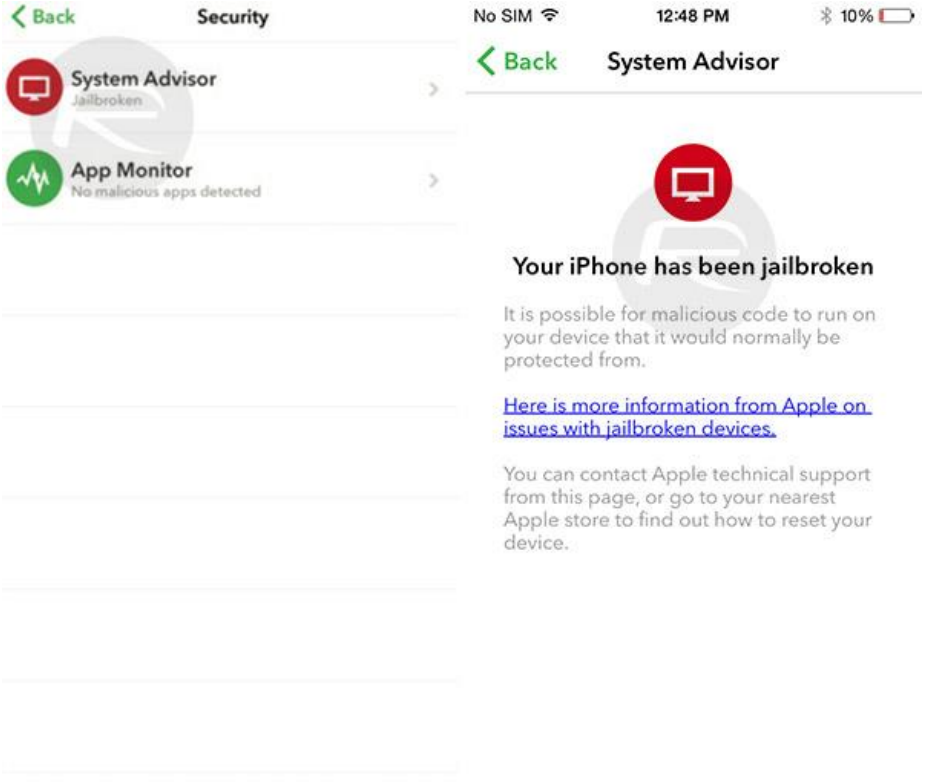
Pero las aplicaciones dañinas no solo afectan a Google, Apple también las tiene que combatir, en 2017 Will Strafach, CEO de Sudo Security Group, realizó un estudio que asegura que App Store posee al menos 76 aplicaciones a disposición de los usuarios que no utilizan el protocolo de seguridad TLS (Transport Layer Security) de tal manera que se pueden interceptar o manipular datos personales de sus usuarios mediante un silencioso ataque man-in-the-middle, aunque estas aplicaciones no contengan código malicioso por

parte de los desarrolladores, otras personas pueden usar estas vulnerabilidades para obtener información personal de sus usuarios y atacarles, por ejemplo, con spam.

Will Strafach avisó a todas las empresas que crearon estas aplicaciones, aunque no pudo contactar con todas ellas por falta de datos de contacto. Esta cifra de aplicaciones es baja, pero acumulan más de 18 millones de descargas por lo que muchos usuarios podrían ser o haber sido afectados.

Las aplicaciones vulnerables pueden clasificarse por los diferentes niveles de riesgo:

- Aplicaciones de riesgo bajo, permiten interceptar datos analíticos parcialmente sensibles sobre el dispositivo y datos personales parcialmente confidenciales como son el correo electrónico del usuario y sus credenciales para iniciar sesión en una red no hostil, en este tipo de redes no se podría realizar un ataque. 33 aplicaciones contienen este tipo de riesgo.
- Aplicaciones de riesgo medio, permiten interceptar credenciales de inicio de sesión y tokens de autenticación de sesión. 24 aplicaciones se engloban en este tipo.
- Aplicaciones de riesgo alto, permiten interceptar credenciales de inicios de sesión de servicios financieros o médicos y tokens de autenticación de sesión. 19 aplicaciones albergan esta vulnerabilidad.



Hemos realizado una búsqueda de las diferentes aplicaciones vulnerables y existen todavía algunas en las cuales podemos interceptar información, otras de las apps que encontró Will Strafach ya han eliminado la vulnerabilidad o no se encuentran en App

Store, debido a que el número de aplicaciones vulnerables a ataques man-in-the middle crece constantemente, solo cito algunas junto con sus datos vulnerables:

- VivaVideo—Free Video Editor & Photo Movie Maker. La versión del sistema operativo, el modelo del dispositivo y las queries de búsqueda.
- Uconnect Access. Las credenciales de esta aplicación, de Pandora y de Slacker Radio del usuario durante su configuración inicial. La API de inicio de sesión confirma que valida correctamente los certificados por lo que es poco probable que un atacante pueda utilizar esta vulnerabilidad para causar problemas a su vehículo.
- Epic!—Unlimited Books for Kids. Las claves de cifrado. Es probable que no haya efectos adversos para el usuario final derivados de la interceptación, ya que las claves tienen una alta probabilidad de estar relacionadas con la gestión de derechos digitales.
- Mico—Chat, Meet New People. La dirección de correo electrónico y la versión del sistema operativo.
- Tencent Cloud. La información del análisis del dispositivo ofuscada.
- Huawei HiLink (Mobile WiFi). El modelo del dispositivo y su versión del sistema operativo.
- VICE News. El modelo del dispositivo, la versión del sistema operativo y las llamadas a la API de terceros.
- Trading 212 Forex & Stocks. El nombre de usuario.
- CashApp—Cash Rewards App. La versión del sistema operativo y el nombre del proveedor de la red del dispositivo que ejecuta la aplicación.
- YeeCall Messenger-Free Video Call&Conference Call. La dirección de correo electrónico y el número de teléfono del usuario.
- Loops Live. Los códigos numéricos para identificar el país y el operador de telefonía móvil.
- Privat24. El modelo del dispositivo y la versión del sistema operativo.
- Private Browser—Anonymous VPN Proxy Browser. Los datos de Facebook Analytics y las llamadas a la API de terceros, y posiblemente más datos que aparecen ofuscados.
- Cheetah Browser. El modelo del dispositivo, la versión del sistema operativo, la localización GPS, y las claves de autocompletado de los motores de búsqueda Google y Baidu.
- AMAN BANK. Las llamadas genéricas a la API. El presidente de este banco de Libia informa de que tienen una nueva aplicación y esta se eliminará próximamente pero todavía podemos encontrarla.
- FirstBank PR Mobile Banking. La llamada a la API de verificación de la versión de la aplicación.
- vpn free—OvpnSpider for vpngate. La lista de servidores VPN y la información del servidor VPN usado. Estos datos se pueden manipular.
- Vpn One Click Professional. La lista de servidores VPN, la información del servidor VPN usado y los enlaces de descarga directa “Mobileconfig”. Estos datos se pueden manipular.
- Lottery.com: Play the Lottery. Las llamadas a la API.
- Foscam Camera Viewer by OWLR. Las llamadas a la API.

- Code Scanner by ScanLife. El modelo del dispositivo, la versión del sistema operativo, los códigos numéricos para identificar el país y el operador de telefonía móvil, y la lista de los sensores beacon.
- Yo. Datos transmitidos a su servidor, entre ellos, nombre de usuario, contraseña, token de autenticación, datos potencialmente sensitivos, tales como, información de contacto.
- EFS Mobile Driver Source. Datos transmitidos a su servidor, entre ellos, el número de tarjeta y el PIN.
- Panda Mobile Security. Datos transmitidos a sus servidores.
- Hay muchas más aplicaciones vulnerables como son: Ellentube, Radio Javan, Dolphin Web Browser –Fast Private Internet Search, Indiana Voters, 21st Century Insurance, BCR Móvil, America's First FCU Mobile Banking, Banque zitouna, Diabetes in Check, PayQuicker, Dollar Bank Mobile, State Bank Anywhere o Space Coast Credit Union Mobile, Think Mutual Bank—Mobile Banking App, de las cuales se pueden interceptar datos transmitidos a sus respectivos servidores, entre ellos, el nombre de usuario y la contraseña.

Will Strafach confirma que ha encontrado sobre 250 aplicaciones vulnerables a este ataque en sus pruebas, y que la cifra crece, por lo que está trabajando en una aplicación (que incluye una versión gratuita) para mitigar esta clase de vulnerabilidad y otras, aprovechando el sistema de análisis y conjunto de datos con el que cuenta, ya que ha podido señalar automáticamente qué aplicaciones específicas son vulnerables con una precisión decente.

Por parte de Apple se desconocen vulnerabilidades en aplicaciones de su tienda ya que ellos se reservan el derecho a divulgar, discutir o confirmar sus problemas hasta que se haya realizado una investigación y se haya solucionado el mismo, mediante parches o posteriores versiones.

De esta forma consiguen parecer la tienda de aplicaciones y el sistema operativo más fiable.

3.2. Antivirus en tiendas de aplicaciones

Como podemos comprobar ninguna tienda de aplicaciones móviles se encuentra libre de las vulnerabilidades que ciberdelincuentes quieren albergar en su software, es por ello por lo que algunas de estas empresas han creado antivirus para combatirlos.

3.2.1. Google Play

Google lanzó en 2017 el antivirus Google Play Protect para proteger tu móvil contra aplicaciones maliciosas de su tienda. Este se encuentra activado por defecto en nuestra cuenta de Google, pero puede ser desactivado desde la plataforma Play Store.

El antivirus comprueba la seguridad de las aplicaciones de Play Store antes de que las descargues, comprueba que en el dispositivo no haya aplicaciones con software malicioso de otras fuentes, y elimina del dispositivo y advierte de las aplicaciones dañinas conocidas.

Esto lo hace con un algoritmo de aprendizaje automático, el cual se entrena con información que envía este antivirus a Google de aplicaciones de fuentes desconocidas instaladas en tu dispositivo, además de las que se intentan albergar en su tienda con software malicioso y son interceptadas o las que se interceptan una vez almacenadas.

3.2.2. App Store

Apple lanzó en 2015 Gatekeeper que protege al dispositivo Mac de aplicaciones maliciosas.

Este software comprueba que la aplicación descargada no tenga software malicioso ya conocido.

Gatekeeper bloquea aplicaciones creadas por desarrolladores de software malicioso, si una aplicación ha sido creada por un desarrollador desconocido (sin ID de Apple) o de software malicioso puede impedir que se instale en el dispositivo.

Este antivirus usa una lista de softwares no permitidos. Cuando se pretende instalar una aplicación que coincide con alguna característica de la lista la identifica y le advierte.

Esta lista se va actualizando conforme se crean nuevas vulnerabilidades.

3.2.3. Microsoft

Microsoft nos proporciona su antivirus Windows Defender que se encuentra instalado en los dispositivos con su sistema operativo más reciente Windows 10. Este nos ofrece una protección a tiempo real en nuestros móviles y PCs, aunque no analiza las aplicaciones de su tienda antes de descargarlas podemos tener nuestros dispositivos libres del software malicioso que ellos detectan y registran en su librería de bases de datos de ficheros y configuraciones con software no deseado.

Windows Defender se está convirtiendo en un antivirus muy valorado pudiendo detectar malwares que se ocultan en memoria y se activan al arrancar el sistema operativo siendo muy difícil su detección y eliminación.

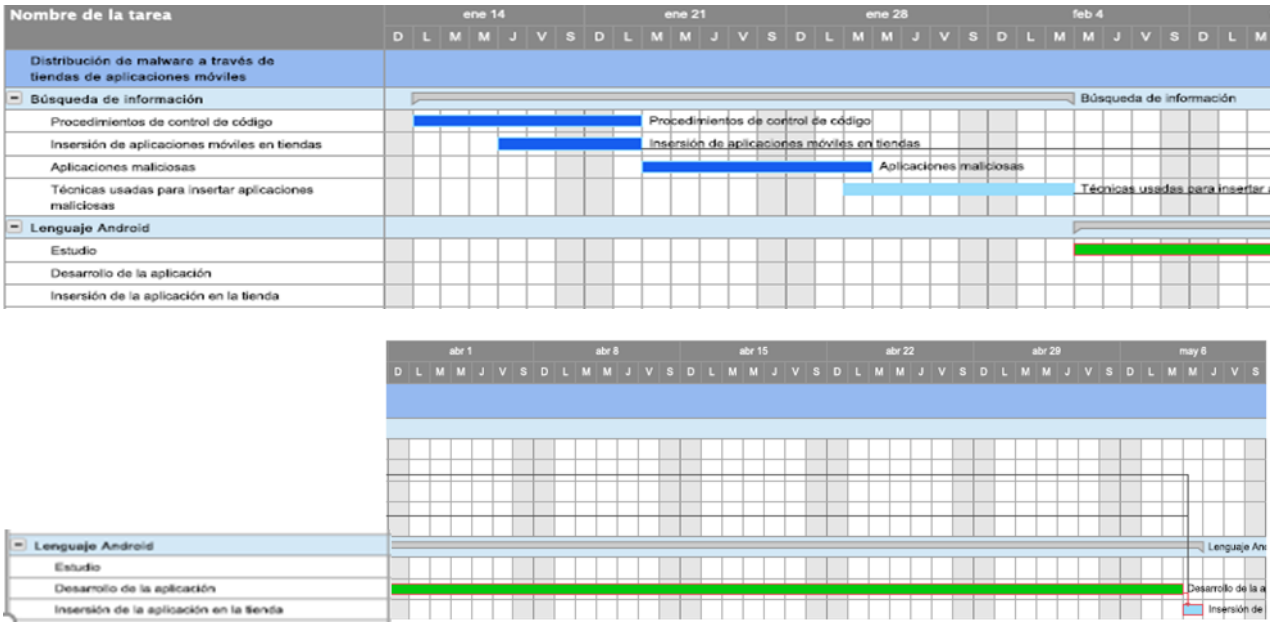
A pesar de que estas empresas estudian continuamente para combatir el software malicioso, encontramos cada día más ciberdelincuentes que investigan formas de introducir malwares en sus tiendas de aplicaciones móviles para obtener beneficios con ellos.

4. Desarrollo

En las secciones que preceden se explicará el proceso que ha seguido el desarrollo del proyecto, y las consideraciones que se han ido teniendo en cuenta en el transcurso de este, siguiendo los objetivos que se expusieron en un principio y a continuación defino brevemente:

- Estudio de los diferentes tipos de malwares.
- Normas y mecanismos de control que realizan las empresas para la detención de estas aplicaciones infectadas.
- Introducir una aplicación infectada con un malware en Play Store.

Para la realización del proyecto se pretendía seguir una planificación inicial de 187 horas que muestro a continuación:



Debido a mi falta de conocimiento sobre la programación en Android esta planificación no la he podido seguir y el número de horas para la realización del proyecto se han duplicado a 310 horas.

Sin embargo, la creación del malware y su inserción en Play Store que es uno de los objetivos más importantes del proyecto ha concluido en menos tiempo del esperado.

La aplicación que se desarrolla en este proyecto tiene el nombre de “RateArt” se trata de una red social donde se podrán ver creaciones de artistas y valorarlas, así como podrás subir imágenes de tus obras para que otros usuarios la valoren.

4.1. Tipos de malwares

El malware, es también conocido como badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información.

El software no deseado está en constante desarrollo, y puede aparecer en programas que queremos mantener en nuestros dispositivos tales como en antivirus.

Estos malwares pueden robar la información personal del usuario, bloquear su PC hasta que pague una cantidad de dinero impuesta por el creador del malware, usar su ordenador para enviar spam o descargar otro software malicioso.

Existen diversas clasificaciones de malwares, dependiendo de la compañía que se dedica a ello, entre estas se encuentran, Microsoft y otras empresas que ofrecen antivirus, por ejemplo, Karpersky. A continuación, se clasificará los diferentes malwares conforme en Wikipedia:

- Malwares infecciosos:

    - Virus: Programa que, al ejecutarse, se propaga infectando otro software ejecutable dentro de la misma computadora. Los virus también pueden tener una carga útil que realice otras acciones maliciosas. Son los usuarios quienes lo transmiten.

      El malware más famoso introducido en App Store se trataba de un virus llamado XCodeGhost.
      Los desarrolladores del virus infectaron el compilador (XCode) que se utiliza para crear las aplicaciones en iOS, por lo que muchos desarrolladores estaban incluyendo código malicioso en sus aplicaciones sin saberlo.
      Las aplicaciones que contuvieron este virus enviaban información personal de sus usuarios a los atacantes, además XCodeGhost conseguía sortear la revisión de las aplicaciones que se suben a la tienda de Apple.
      Este virus ha estado albergado en App Store desde 2008 hasta 2015, cuando unos desarrolladores chinos de iOS lo descubrieron.

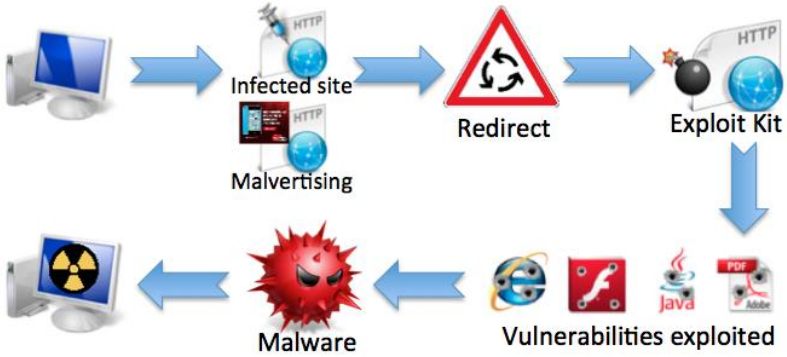
    - Gusanos: Se caracterizan por propagarse a sí mismos, a diferencia de los virus que son propagados por los usuarios, lo que consiguen mediante correos electrónicos, aplicaciones de mensajería instantánea, programas de compartición de archivos, redes sociales o explotando vulnerabilidades en una red de computadoras para infectar otros equipos. Estos malwares pueden contener instrucciones maliciosas, por ejemplo, pueden borrar archivos.

- Malwares ocultos:

- Puertas traseras: Programas que eluden los procedimientos de autenticación al conectarse a una computadora permitiendo a piratas informáticos el acceso y control del PC.

Uno de los malwares más famosos introducidos en Play Store se trata de una puerta trasera llamada Ztorg, el cual se ha introducido más de 100 veces en la tienda de Google y ha infectado a más de un millón de usuarios. Los atacantes consiguieron introducir el malware en Play Store subiendo una versión limpia de la app y parcheándola, introduciéndole el código malicioso, posteriormente.
Este malware tomaba el control del dispositivo realizando diversas acciones como enviar SMS premium al número del atacante mientras silenciaba el móvil y borraba el registro de mensajes para que el usuario no pudiera detectar nada.
A mediados de 2017, fue la última vez que se detectó el virus por la empresa Kaspersky en una aplicación que servía de guía para el juego Pokémon Go.
Google borró todas las aplicaciones que contenían el código malicioso.

- Drive-by download: Se trata de páginas que descargan automáticamente en los equipos de sus usuarios, sin que ellos se percaten, spywares o códigos que les dan a los propietarios de estas webs información sobre el equipo.



- Rootkits: Técnicas usadas para modificar el sistema operativo de un ordenador para permitir que el malware permanezca oculto al usuario,

ocultando el fichero que lo contiene en el explorador de archivos y el proceso que ejecuta en la lista de procesos del sistema.

- Troyanos: Programas maliciosos que parecen atractivos e invitan al usuario a ejecutarlo.
  Ese software, puede tener un efecto inmediato y puede llevar muchas consecuencias indeseables, por ejemplo, borrar los archivos del usuario o instalar más programas indeseables o maliciosos.

Los tipos de troyanos son: backdoors, banker, botnets, dialer, dropper, downloaders, keylogger, password stealer, proxy.

- Malwares para obtener beneficios:

Los programas maliciosos pueden ser creados como una forma de vandalismo o travesura, o, como la mayoría del software malicioso, con un fin económico o para obtener beneficios en algún sentido.
Se pueden obtener beneficios pagándoles a empresas por mostrar su publicidad a diversos usuarios o proporcionándoles correos electrónicos robados para que ellas mismas les muestren su publicidad, cifrándoles archivos a los usuarios para

pedirles dinero para su recuperación o chantajeándolos de otras formas. A continuación, explicaremos como se usan ciertos malwares para obtener ingresos:

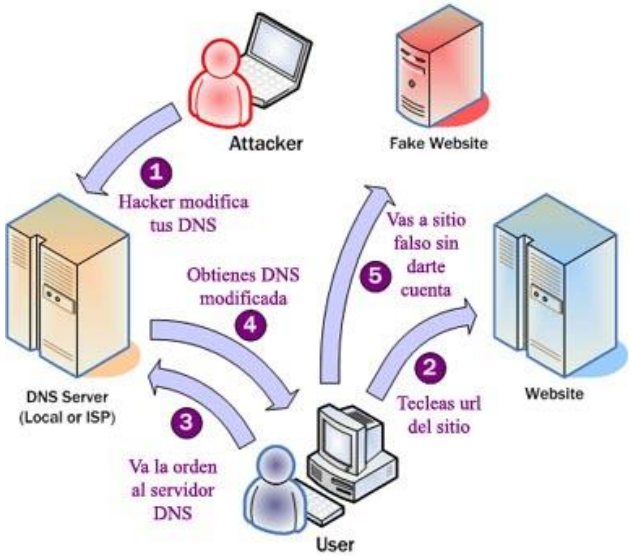
- Spyware, adware y hijacking: Con ellos se puede mostrar publicidad:

  Los spywares como bien su nombre nos indica son programas espías, tienen como objetivo recopilar información del equipo en el que se encuentra y transmitírselo a quien lo ha introducido, por lo que sirven para recopilar información sobre las actividades realizadas por un usuario, como las páginas webs que visita o las direcciones de correo electrónico. Con esta información se puede obtener beneficios distribuyéndola a agencias de publicidad u otras organizaciones interesadas que se encargan de enviarles spam a los usuarios afectados.
  Estos programas se pueden ocultar tras software deseable descargado de internet, pueden recoger la información mediante cookies de terceros o mediante barras de herramientas instaladas en navegadores web por lo que el usuario raramente se percata de ello.
  Los autores de spyware que intentan actuar de manera legal se presentan abiertamente como empresas de publicidad e incluyen unos términos de uso, en los que se explica de manera imprecisa el comportamiento del spyware, que los usuarios aceptan sin leer o sin entender.
  Entre otros delitos estos softwares pueden provocar robos bancarios, suplantaciones de identidad y robo de información.

  Los programas adware son softwares publicitarios, muestran publicidad al usuario de forma intrusiva en forma de ventana emergente (pop-up) o de cualquier otra forma, pueden aparecer en páginas webs, durante la instalación de algún programa o en el equipo si se ha instalado el programa que lo contiene. Algunas veces son programas llamados shareware los que contienen el software malicioso, estos permiten usar el programa de forma gratuita a cambio de publicidad, la cual desaparece al pagar cierta cantidad, por lo que el usuario es consciente de la misma. Esta publicidad aparece inesperadamente en el equipo y resulta muy molesta.

Los hijackers son programas que intentan adueñarse o robar algo en otro sistema, contemplan el robo de información, el secuestro de conexiones de red, de sesiones de terminal, servicios, módems, etc., en este apartado en el cual estamos enfocados a los softwares para mostrar publicidad, ellos realizan cambios en la configuración del navegador web, pueden cambiar la página de inicio del navegador por páginas web de publicidad, redireccionar los resultados de los buscadores hacia anuncios de pago o páginas de phishing bancario.

El pharming es una técnica que suplanta al DNS, modificando el archivo hosts, para redirigir el dominio de una o varias páginas web a otra página web, muchas veces una web falsa que imita a la verdadera. Esta es una de las técnicas usadas por los hijackers o secuestradores del navegador de Internet. Esta técnica también puede ser usada con el objetivo de obtener credenciales y datos personales mediante el secuestro de una sesión.



- Keyloggers y stealers. Se usan para robar la información personal de los usuarios afectados.

Cuando un software produce pérdidas económicas para el usuario de un equipo, también se clasifica como crimeware o software criminal. Estos programas están encaminados al aspecto financiero, la suplantación de personalidad y el espionaje.

Los keyloggers y los stealers son programas maliciosos creados para robar información sensible. El creador puede obtener beneficios económicos o de otro tipo a través de su uso o distribución en comunidades underground, a estas comunidades pertenecen expertos en informática y se agrupan por ideologías, hackers, crackers, phreackers o virus writers, con el fin de ampliar sus conocimientos.

Los keyloggers monitorizan todas las pulsaciones del teclado y las almacenan para un posterior envío al creador, pueden ser dispositivos hardwares soldados en el teclado o conectados entre el cable del teclado y el ordenador, o dispositivos softwares, algunos se albergan en el núcleo del sistema operativo, y así podrían actuar, por ejemplo, como driver del teclado.

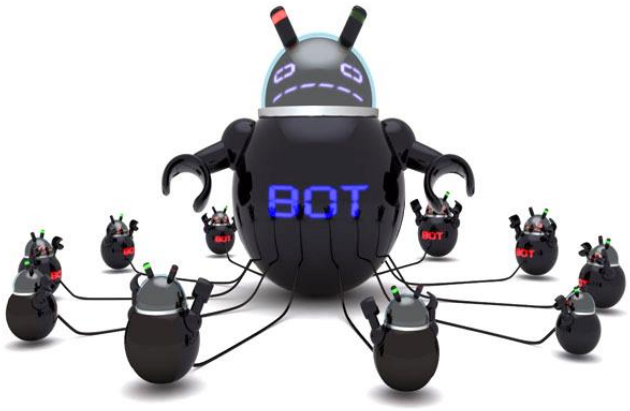
Si las contraseñas se encuentran recordadas en el equipo, de forma que el usuario no tiene que escribirlas, el keylogger no las recoge, eso lo hacen los stealers. La mayoría los keyloggers son usados para recopilar contraseñas de acceso, pero también pueden ser usados para espiar conversaciones de chat u otros fines.

Los stealers roban información privada pero solo la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas recordadas, por ejemplo, en los navegadores web o en clientes de mensajería instantánea, descifran esa información y la envían al creador.

- Dialers: Se usaban para realizar llamadas telefónicas.
  Los dialers son programas maliciosos, muy populares cuando se usaban los módems dial-up, ya que tomaban el control de estos realizando

llamadas a números de teléfonos con tarificación especial, muchas veces internacional, y dejaban la línea abierta cargando el coste de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos, salva pantallas, pornografía u otro tipo de material.

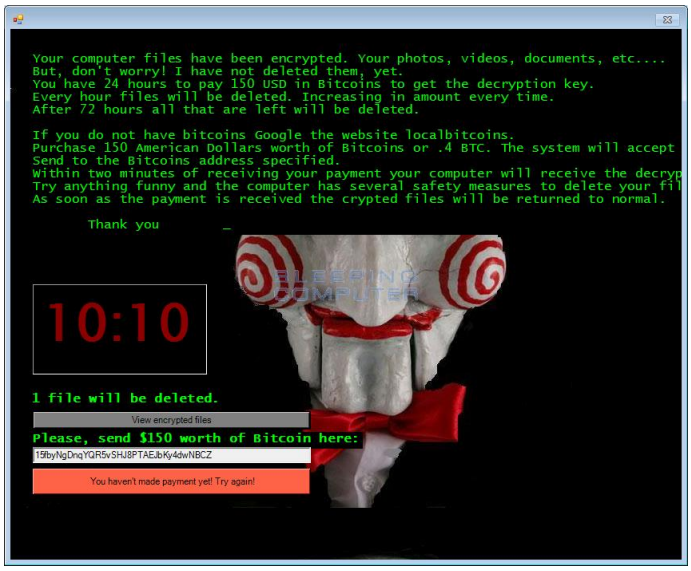
- Botnets: Se usan para lanzar ataques distribuidos.
  Las botnets son redes de computadoras infectadas, también llamadas "zombis", porque pueden ser controladas a la vez por un individuo y realizan distintas tareas.
  A diferencia de con otros tipos de malwares, el beneficio es mayor usando botnets ya que se están usando muchos ordenadores para ese fin, por ejemplo, se pueden usar para el envío masivo de spam o para lanzar ataques DDoS contra organizaciones como forma de extorsión o para impedir su correcto funcionamiento.
  La ventaja que ofrece a los spammers el uso de ordenadores infectados es el anonimato, que les protege de la persecución policial.



  En una botnet cada computadora infectada por el malware se loguea en un canal de IRC u otro sistema de chat desde donde el atacante puede dar instrucciones a todos los sistemas infectados simultáneamente. Las botnets también pueden ser usadas para actualizar el malware en los sistemas infectados manteniéndolos así resistentes ante antivirus u otras medidas de seguridad.

- Rogue Software:
  Estos malwares hacen creer al usuario que está infectado por un malware, con lo cual intentan que el usuario pague por un programa inútil o que se descargue un software malicioso.

- Ransomware:
  También llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un rescate para poder recibir la contraseña que permite recuperar los archivos.



Desde un primer momento estaba pensado que la aplicación albergara este último tipo de malware, un ransomware, aunque con el paso del tiempo y la dificultad que tenía en el manejo de archivos con Android pensé en otra posibilidad la de crear un adware que abriera ventanas continuamente.

Finalmente, la aplicación maliciosa que se alberga en Play Store contiene un ransomware que encripta en el dispositivo móvil la foto que se sube a la aplicación.

En el siguiente apartado se exponen las normas de seguridad que se deben llevar a cabo para alojar una aplicación en las diferentes plataformas de aplicaciones móviles.

4.2. Normas y mecanismos de control de seguridad

Las tiendas de aplicaciones disponen de una serie de normas para que puedas alojar tu aplicación en ellas, todas las tiendas comprueban que la aplicación que se ha subido respeta las siguientes normas, aparte de la legislación local del país en el que la aplicación está disponible.

	ANDROID	IOS	MICROSOFT
CONTENIDO RESTRINGIDO			
Contenido ofensivo, insensible, difamatorio, discriminatorio, sobre acoso, violencia, odio, etc.			
Contenido sobre personas o animales siendo asesinados			
Facilitar el uso o la compra de armas			
Contenido sexual			
Contenido sobre comentarios religiosos inflamatorios o citas de textos religiosos engañosas			
Información falsa			
Funcionalidad trucada			
Activan llamadas anónimas o bromas telefónicas			
Acontecimientos de carácter delicado o trágico, que traten sin sensibilidad a un desastre natural, atrocidad, conflicto, fallecimiento, etc			
Juegos de apuestas en España			

De esta parte se puede destacar la App Store que mientras otras tiendas permiten aplicaciones de bromas telefónicas, esta restringe este tipo de aplicaciones.

Los usuarios crean contenido en algunas aplicaciones sobre todo en redes sociales, en la política de uso de las aplicaciones que alberguen este contenido debemos reflejar una serie de normas, entre ellas el contenido bloqueado para cada tienda:

	ANDROID	IOS	MICROSOFT
CONTENIDO GENERADO POR EL USUARIO			
Contenido ofensivo			
Usuarios abusones			
Bullying			
Mostrar contenido sin filtro por el usuario			
No cumple la política			

En Play Store las aplicaciones deben definir qué contenido se considera inadecuado y prohibirlo mediante condiciones de uso o política que deben aceptar sus usuarios, se debe implementar un sistema de notificación de uso inadecuado fácil de utilizar para el usuario, que permita retirar el contenido que infrinja las condiciones de forma eficaz, se debe eliminar o bloquear a los usuarios ofensivos y proporcionar una categorización correcta para la aplicación.

En Microsoft Store, sin embargo, es el propio usuario de la aplicación el que debe definir qué contenido desea que se le muestre o cuál no.

Estas normas no se cumplen siempre, existe una aplicación muy famosa llamada Twitter que no censura ningún tipo de contenido, ya sea de índole sexual, violenta o de bullying, casos de bullying mediante redes sociales se emiten en los telediarios frecuentemente, y no se retiran estas aplicaciones.

También debemos tener especial precaución con las aplicaciones recomendadas principalmente al sector de los niños. Las normas que debemos cumplir para albergar una aplicación en esta categoría son las siguientes:

	ANDROID	IOS	MICROSOFT
CATEGORÍA DE NIÑOS			
Enlaces exteriores de la aplicación			
Compra de oportunidades			
Distracciones pensadas para padres			
Anuncios no apropiados			
No cumple con la Ley de Protección de la Privacidad Infantil en Internet			
Abuso sexual infantil			

Todas las aplicaciones como también es dictado por la ley no permiten el abuso sexual infantil, aunque se siguen cometiendo delitos de esta índole en redes sociales albergadas en las diferentes tiendas de aplicaciones móviles.

Las aplicaciones juegan en casi todos los casos con la psicología de las personas, pero en los casos más extremos puede dañarles su salud, es por lo que se prohíben en algunas tiendas cierto tipo de aplicaciones:

	ANDROID	IOS	MICROSOFT
DAÑO FÍSICO			
App médicas que proveen datos inadecuados			
Fomentar el consumo de tabaco, drogas o alcohol			
Mostrar controles de alcoholemia			
Falsa información de contacto			
Facilitar compra o venta de drogas			

Aunque se prohíba fomentar el consumo de alcohol encontramos una aplicación en la Play Store de Android y en la App Store de iOS, muy famosa entre los jóvenes, llamada “Picolo” que contiene diversos juegos que incitan a beber.

Para todas las tiendas de aplicaciones es muy importante su seguridad y todas advierten de que una aplicación para ser subida a su plataforma no debe contener ningún tipo de malware, ni se debe cambiar o extender la funcionalidad de la aplicación con código dinámico para que lo contenga.

En este proyecto nos saltaremos esta norma de seguridad he introduciremos un malware en Play Store.

Por otra parte, debemos exponer condiciones generales como son la protección de datos esta norma es muy importante debido a la ley LOPD, siendo sancionada aquella persona que la incumpla.

Facebook, una aplicación de las más descargadas de todas las tiendas, ha incumplido esta norma ya que ha estado almacenando sin el conocimiento de los usuarios, sus registros de llamadas y de mensajes, así ha podido comprobarlo un hombre llamado Dylan McKay descargando un archivo de sus datos de Facebook.

Facebook respondió explicando que pedían permiso para acceder a los contactos del teléfono para actualizarlos y, también, para usarlos para su algoritmo de búsqueda de amigos.

En algunas versiones de la aplicación de mensajería Messenger creada por Facebook podían acceder a los registros de llamadas y mensajes, aunque se hubieran denegado los permisos que la aplicación pide para obtenerlos debido a la forma en la que Android ha manejado los permisos para acceder a los registros de llamadas en el pasado, exactamente hasta su versión 4.1.

Además, está prohibido en todas las plataformas la suplantación de identidad y propiedad intelectual como dicta la ley de derechos de autor, por lo tanto, quedan prohibidas acciones como las siguientes, usar contenido ajeno del cual no se tiene licencia para usarlo, usar marcas patentadas sin permiso, contenido con copyright, representaciones falsas de aplicaciones que se puedan confundir con las originales, compartir ficheros de descarga de audio o video sin autorización, sugerir que la tienda de aplicaciones en la que se alberga avala la aplicación o imitar un producto.

En todas las plataformas de aplicaciones móviles se prohíbe usar o transmitir datos del usuario sin su consentimiento, es decir se debe pedir permisos para acceder a sus datos como son su localización, sus contactos, su calendario, etc., tampoco se deben pedir datos personales para funcionar, usar la aplicación para averiguar credenciales o datos privados, rastrear usuarios sin su consentimiento, compartir datos con terceras partes a no ser que sea para obtener mejoras en la aplicación, ni coleccionar, almacenar o transmitir datos de forma insegura, es decir, sin cifrarlos.

Aparte de las normas expuestas anteriormente que tienen en cuenta casi todas las plataformas de aplicaciones móviles, la App Store de iOS hace hincapié en otras normas respectivas a los datos sobre salud de los usuarios, prohíbe usar o revelar datos de salud

o investigaciones médicas, escribir datos falsos o inapropiados y almacenar información médica personal en la nube.

Microsoft prohíbe almacenar datos sobre la salud personal si no es el principal objetivo de la aplicación y si no tiene el consentimiento del usuario, pero Apple es más restrictivo.

Las consecuencias que se deben asumir por saltarse estas normas son la eliminación de la aplicación de la plataforma, llegando a ser posible la eliminación de la cuenta del desarrollador, e incluso tienen procedimientos para detectar si el desarrollador crea otra cuenta y lo vetan de la tienda de aplicaciones.

Después de comparar las diferentes normas en las tiendas de aplicaciones podremos pensar que tiene la misma complejidad a la hora de introducir un malware u otro tipo de contenidos, pero no es verdad, ya que después de entrevistar a desarrolladores de aplicaciones para las distintas plataformas, nos comentan que Apple revisa el código manualmente, e incluso llama por teléfono al desarrollador para sugerirle mejoras de la aplicación, lo cual no se produce ni con Google ni con Microsoft pudiendo entender que la App Store de iOS alberga las aplicaciones más seguras.

Una vez hemos estudiado los diferentes tipos de malwares, cómo se han introducido en las tiendas de aplicaciones y las consecuencias que tiene introducirlos, se procede a explicar el desarrollo de la aplicación maliciosa y cómo es introducida en Play Store.

4.3. Aplicación maliciosa

Con el fin de demostrar si es fácil insertar un virus en Play Store y a su vez infringir la norma de seguridad que lo prohíbe, en este apartado se desarrollaran los pasos para la creación de una aplicación maliciosa y su posterior inserción en Play Store.

Empezaremos por explicar los requisitos importantes de la aplicación que se ha creado en el siguiente subapartado.

4.3.1. Requisitos de la aplicación

El objetivo de la aplicación es que contenga un código malicioso el cual no vulnere ninguna ley, como hemos podido apreciar en el apartado donde se explicaban los diferentes tipos de malwares, la mayoría de ellos sirven para extraer información personal de los usuarios con lo cual si insertáramos un virus de ese tipo estaríamos vulnerando la ley de Protección de Datos, ya que no pedimos permisos a los usuarios para que nos lo proporcionen.

Los malwares que, en un primer momento, podrían ser más factibles a la inserción, teniendo menos efectos nocivos ante la ley son adware o ransomware.

Para insertar un ransomware, lo ideal sería que la aplicación manejara archivos, además la aplicación deberá tener funcionalidad y ser atractiva para que, en caso de que se le realicen pruebas, sea más compleja su detención y no arriesgarnos meramente a insertar un malware en Play Store que nos puedan detectar con sólo iniciar sesión en la aplicación.

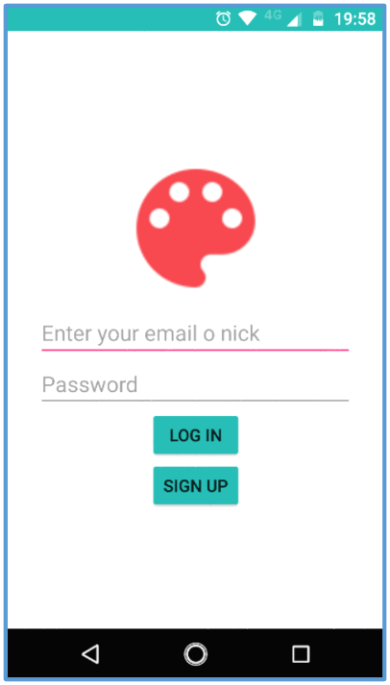
La creación de la aplicación se enfocará en que esta sea factible para la inserción de un ransomware, es decir, se debe pedir permisos para acceder al almacenamiento interno del dispositivo sin que sea sospechoso. Esta aplicación también serviría para la creación de un adware en caso de ser necesario, ya que en todas las aplicaciones se podrían usar permisos para enviar notificaciones sin que fuera sospechoso para el usuario. A continuación, se explican los requisitos funcionales que debe cumplir la aplicación.

- La aplicación debe registrar los siguientes datos de usuarios, nombre, apellidos, email, nick, contraseña. Los usuarios iniciarán sesión en la aplicación usando el email o nick y la contraseña.
- La aplicación contará con posts los cuales estarán formados por una imagen, un título y una descripción. Los usuarios podrán añadir posts a la aplicación cuantos quieran.
- Los usuarios podrán valorar los posts de otros usuarios con un valor de 0 a 5.
- Los usuarios podrán ver estadísticas propias: El número de posts que han subido, el detalle de cada post junto con la media de valoraciones que tiene entre todos los usuarios del sistema, la media de las valoraciones medias de todos sus posts y la posición en el ranking entre todos los usuarios, siendo el usuario primero en el ranking aquel que cuenta con una media más alta de entre todas las medias de sus posts.

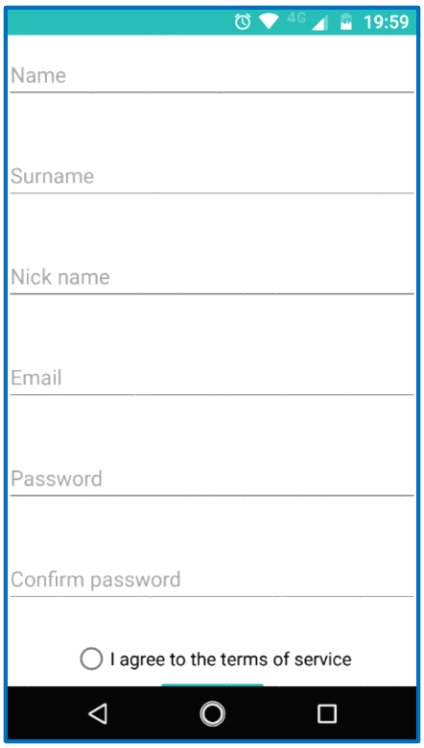
Una vez expuestos los requisitos que debe cumplir la aplicación, se realiza, a continuación, veremos el diseño de esta.

4.3.2. Mockups de la aplicación

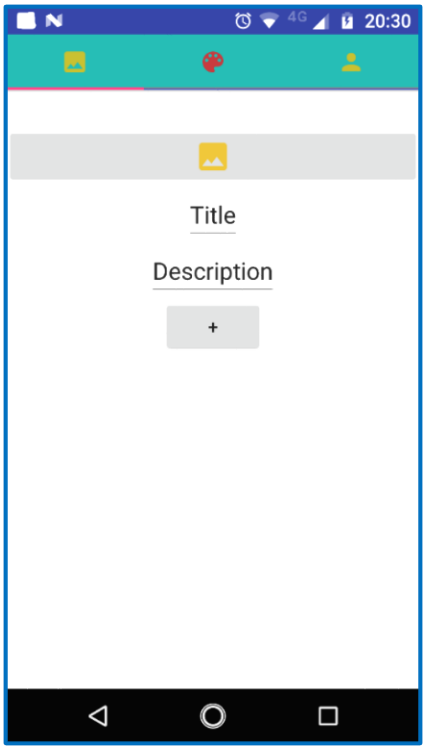
La aplicación, llamada RateArt, tendrá una actividad principal con la que nos podremos registrar e iniciar sesión en la misma:



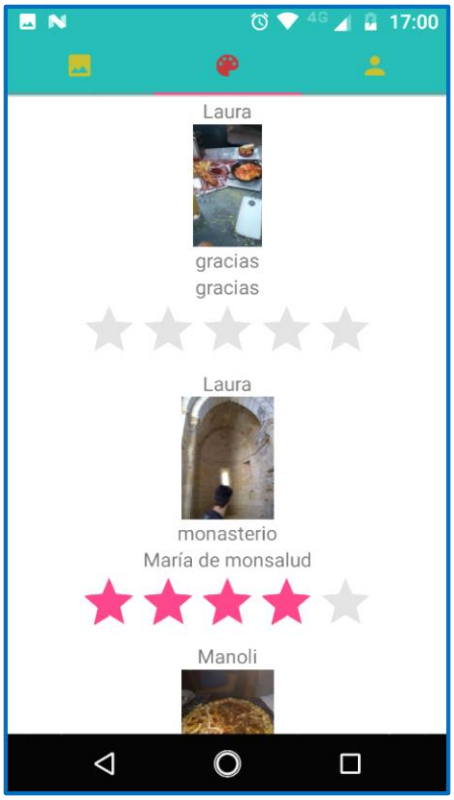
Al pulsar el botón “Sign up” pasamos a la actividad de registro.



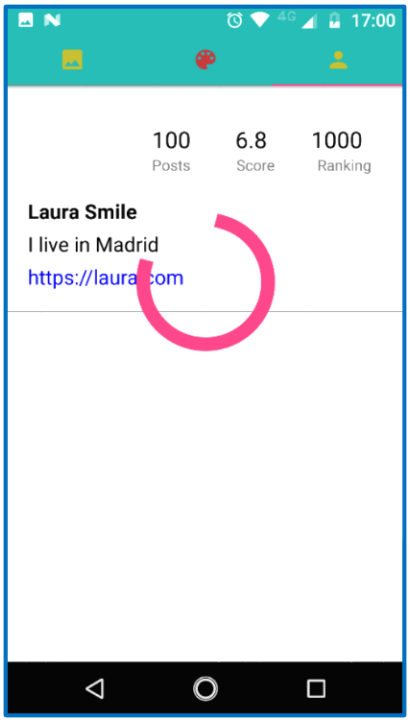
Al iniciar sesión en la aplicación, se nos muestra la pantalla para subir imagen.



Podemos observar en la imagen que cuenta con una barra superior con 3 iconos cada uno de ellos muestra una pantalla distinta, las cuales llamaremos fragmentos.
En el fragmento del icono de la paleta roja veremos los posts subidos por los usuarios de la aplicación, los cuales podremos valorar, incluso los propios.



Por último, en el icono amarillo donde aparece la forma de un avatar, podremos ver estadísticas propias, nuestra información y nuestros posts.



A continuación, vamos a enumerar y explicar brevemente la tecnología con la que se ha desarrollado la aplicación.

4.3.3. Tecnologías usadas para la realización de la aplicación

En este apartado se explican brevemente las últimas versiones de las tecnologías usadas para el desarrollo de la aplicación:

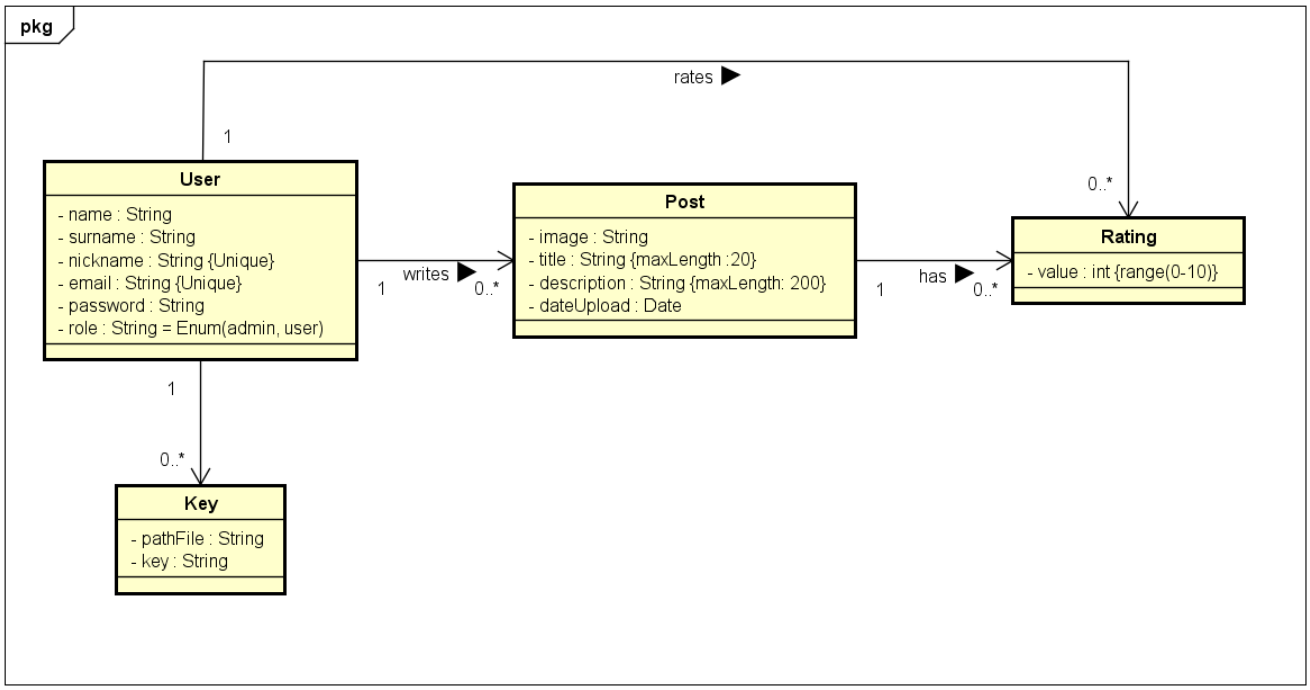
- MongoDB, como base de datos.
- La versión actual, 3.1.2, de 'Android Studio' como entorno de desarrollo.
  Android Studio es el entorno de desarrollo oficial para aplicaciones Android ya que ofrece numerosas herramientas que nos aventajan para construir la aplicación más rápido y con buena calidad, entre ellas podemos mencionar, el editor visual para el diseño, la herramienta Android Virtual Device (ADV) con la cual podemos simular en nuestro ordenador un dispositivo Android para probar nuestra aplicación, el sistema de compilación basado en Gradle flexible, el entorno unificado en el que se pueden realizar desarrollos para todos los dispositivos Android, la herramienta Instant Run para aplicar cambios en la aplicación mientras esta se ejecuta sin la necesidad de compilar un nuevo APK, la integración de plantillas de código y GitHub para ayudarte a compilar funciones comunes de las apps e importar ejemplos de código, las herramientas Lint para detectar problemas de rendimiento, usabilidad, compatibilidad de versión, etc.
  Además, cuenta con más herramientas y frameworks de prueba.
- La versión 8 de Java, JDK 8 como lenguaje de programación del cliente Android, se han usado las siguientes librerías:
  - "Volley" para el envío de las peticiones HTTP al servidor.
  - "Multipart" para el envío de peticiones HTTP al servidor con diferentes tipos de datos, esta librería se ha usado para poder enviar imágenes al servidor, lo cual se intentó realizar con "Volley" pero no fue factible ya que no permite trabajar con datos de gran tamaño ni con objetivos compuestos de múltiples partes pues los guarda en caché.
  - "Glide" para cargar imágenes.
    En un principio se usaba "Universal Image Loader" para cargar las imágenes en vistas de tipo NetworkImageView pero no funcionaba correctamente ya que las imágenes debían ser del mismo tamaño,

- Sublime, como editor de texto para el backend.
- Javascript, como lenguaje de programación del backend con el entorno de ejecución "Node.js" y sus módulos:
  - "Mongoose" para la conexión con la base de datos MongoDB.
  - "Express" para poder usar middlewares y comunicarnos con el cliente
  - "body-parser" para parsear las solicitudes entrantes del cliente en formato JSON.
  - "multer" para poder recibir y enviar ficheros del cliente.
  - "read-chunk", "file-type" y "fs" para poder leer imágenes y devoverlas desde el servidor.
  - "jwt-simple" para crear tokens para la autorización de los usuarios.

Una vez hemos visto, la tecnología que se usará para el desarrollo de la aplicación vamos a explicar los detalles de la implementación.

4.3.4. Modelo conceptual

El backend de la aplicación está implementado en Node.js y usa una base de datos NO-SQL MongoDB, a continuación, podéis ver un diagrama relacional de colecciones y campos.



Finalmente, a la aplicación se le ha insertado un código malicioso con un ransomware, por lo que la base de datos tiene 4 colecciones:

- User: Recoge los datos de cada usuario.
- Post: Cada post consta de un título, una descripción, una imagen y una fecha de creación para ordenarlos en orden descendiente por este último atributo a la hora de mostrarlos en la aplicación.
- Rating: Cada usuario podrá valorar todos los posts una única vez.
- Key: Almacena los datos necesarios para desencriptar las imágenes, estos son, la ruta de la imagen encriptada, la clave de encriptación y el usuario al que se le ha encriptado el archivo.

En el siguiente apartado se explicarán los detalles de la inserción del malware.

4.3.5. Malware insertado en la aplicación

La aplicación se encuentra infectada por un ransomware, su inserción ha sido mucho más fácil de lo que se preveía, ya que java nos provee un paquete llamado "javax.crypto", que contiene varias clases que nos evitan tener que crear algoritmos.

A continuación, explicaremos el proceso que hemos seguido para la creación del malware.

En primer lugar, debemos leer la imagen y devolverla en un array de bytes para su posterior cifrado.
Esto lo conseguimos con la clase InputStream que nos permite abrir un fichero en bytes, y tiene su propio método read para recorrerlo.

Posteriormente se crea una clave de cifrado con la cual debemos cifrar la imagen, con la clase SecureRandom creamos una contraseña aleatoria de cifrado y con la clase KeyGenerator creamos una clave, un tipo llamado SecretKey que nos proporciona la librería de criptografía de Java, con un algoritmo de cifrado simétrico llamado "AES".

Luego creamos un método que encripte la imagen, para ello utilizamos una clase llamada Cipher, le pasamos la clave y la imagen y nos devuelve un array de bytes, el cual es la imagen encriptada.

Finalmente creamos un fichero y guardamos la imagen encriptada.

Fragmento de código mediante el cual se encripta la imagen:

```
public static byte[] encodeFile(SecretKey yourKey, byte[] fileData) throws Exception {

        byte[] encrypted = null;
        byte[] data = yourKey.getEncoded();

        SecretKeySpec skeySpec = new SecretKeySpec(data, 0, data.length,
    algorithm);

        Cipher cipher = Cipher.getInstance(algorithm);
        cipher.init(Cipher.ENCRYPT_MODE, skeySpec, new IvParameterSpec(
            new byte[cipher.getBlockSize()]));
        encrypted = cipher.doFinal(fileData);
        return encrypted;
}
```

Ya tenemos la imagen codificada, llega el turno de eliminar la imagen original, Java también nos proporciona un método para ello que pertenece a la clase File, soló debemos proporcionarle una cadena con la ruta de la imagen original.

Fragmento de código mediante el cual se borra la imagen:

```
private void deleteOriginalImage(){
        File file = new File(filePath).getAbsoluteFile();
        if(file.exists()){
                file.delete();
        }
}
```

Por último y no menos importante, debemos crear un código para decodificar la imagen ya que, si no, no sería un ransomware.

En la base de datos se almacena la clave de encriptación, el usuario y la ruta de la imagen codificada al guardarla en el dispositivo.

Decodificar el archivo es similar a codificarlo usando el método contrario.

Para ello leemos esta vez el archivo codificado, obteniendo un array de bytes, y volvemos a utilizar la clase Cipher esta vez para desencriptar la imagen y guardarla.

Linea de código diferente al procedimiento de encriptar:

```
cipher.init(Cipher.DECRYPT_MODE, yourKey, new IvParameterSpec(new
byte[cipher.getBlockSize()]));
```

Una vez que hemos visto como se ha creado e introducido el malware en la aplicación, veremos los problemas que hemos encontrado en el desarrollo de la aplicación y los cambios que nos han surgido.

4.3.6. Cambios en la aplicación

Una vez realizada la funcionalidad de la aplicación, con un diseño muy pobre se han realizado cambios en la misma, a fin de que sea más atractiva:

- La aplicación se inicializa con una pantalla de splash la cual tiene una duración de dos segundos, donde aparece el logo de la aplicación.
- Los colores principales de la aplicación se han modificado de verde agua y rosa a azul y rojo.
- Al iniciar la aplicación, en la pantalla que se muestra, se añade el logo y firma de la aplicación en la parte superior y en el pie de página, respectivamente, además se escribe texto al lado de los botones, de acceso y registro, siguiendo la misma línea que las aplicaciones de hoy en día
- En la pantalla de registro se cambia el tipo de vista de edición de los textos, EditText a TextInputLayout, con esto conseguimos que se muestren los errores de validación a tiempo real debajo de la caja de texto, también se añade una propiedad para ocultar o mostrar la contraseña, por último, se muestran el logo de la aplicación y la firma como en la pantalla explicada anteriormente.
- Al iniciar sesión en la aplicación, se modifican los botones de la barra superior, ya que no eran llamativos, y los colores de las letras sobre fondo de color a blanco para que resalten, por otro lado, en vez de abrir el fragmento que sirve para la subida de post (fragmento de la izquierda) se cambia para abrir el fragmento donde se muestran todos los posts de los usuarios (fragmento del centro).
- En el fragmento de subida de post, se modifica la imagen del botón para que aparezca más grande y sobre fondo blanco.
- En el fragmento donde se muestran todos los posts de los usuarios, se agrandan las imágenes y se pone información sobre la barra de estrellas para valorar.
- En el fragmento de nuestro perfil (fragmento de la izquierda), se ha quitado la información personal no relevante para nuestra aplicación ya que los demás usuarios solo ven nuestro nick y se ha creado un botón para cerrar sesión.

Con respecto a la funcionalidad, en la primera versión de la aplicación no se guardaban los credenciales del login de la aplicación, con lo cual cada vez que se iniciaba la aplicación nos debíamos loguear, ahora hemos utilizado una clase de Android llamada “SharedPreferences”, que sirve para guardar en un archivo en el dispositivo información con respecto al uso de la aplicación, aquí se almacena nuestro token, pudiendo entrar en la aplicación sin pasar por la pantalla de iniciar sesión y se limpia una vez le damos al botón de cerrar sesión que se encuentra en la pantalla de nuestro perfil, al pulsar a este botón volveremos a la pantalla de login.

Otra parte que en una primera versión no da buena impresión y se debía mejorar eran la vista de las imágenes, las cuales se veían muy pequeñas, porque daban fallos de memoria si se ponían todas a tamaño real, para posicionarlas en la pantalla se utilizaba la librería “UniversalImageLoader” con el tipo de vista de imagen “NetworkImageView”. Ahora para solventar este problema se cambia la librería “UniversalImageLoader” por la librería “Glide”, como recomienda Google para aplicaciones Android, con el tipo de vista de imagen “ImageView”, así podremos extender las imágenes al ancho que tenga la pantalla

con la altura correspondiente para que estas no se vean deformes manteniendo las proporciones.

A la hora de cargar las imágenes también daba problemas de memoria y la aplicación se cerraba al cargar la última imagen, para resolver este problema se pensó en hacer paginación, pero debía modificar varios ficheros y no sabía cuánto iba a tardar ni tenía tiempo, como no era un objetivo de la aplicación se resuelve acortando la petición a 20 imágenes.

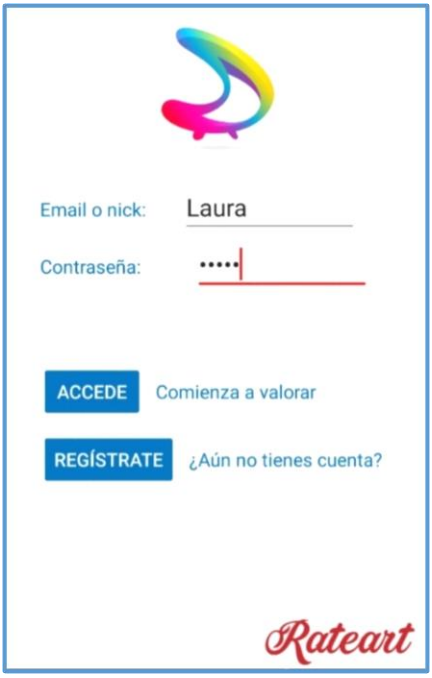
Mostrar los posts propios y poder votarlos en el fragmento del centro, donde se ven todos los posts subidos por todos los usuarios, causó un problema, pues este fragmento no se recargaba al subir un post, después de investigar la manera en la que se podría solventar, no se encontró solución, en cambio el fragmento de la izquierda, donde se ven nuestros posts y estadísticas, sí se recarga automáticamente, por lo que se restringe a que los posts propios solo aparezcan en el fragmento de tu perfil, lo que conlleva a no poder votarlos.

4.3.7. Diseño final

A continuación, se muestran capturas de pantalla de las diferentes layouts que componen la aplicación.

Al arrancar la aplicación podremos ver una pantalla de presentación donde se muestra el logo y el nombre de la aplicación.

Esta pantalla, la cual podremos observar durante dos segundos, da paso a una actividad donde podremos iniciar sesión o registrarnos.



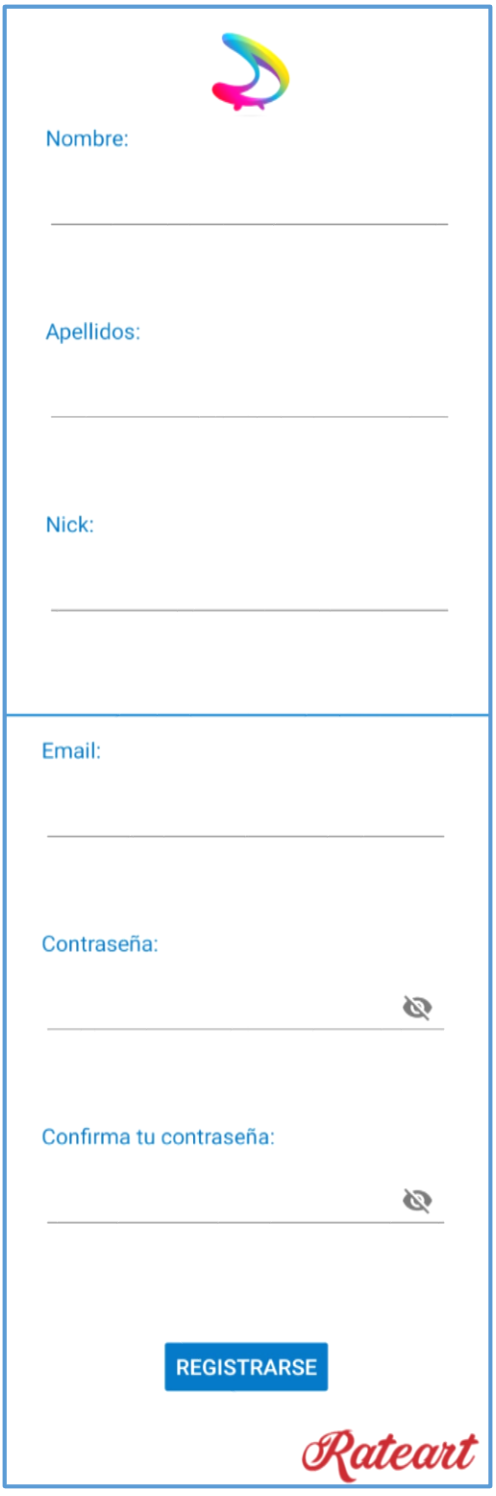
En esta pantalla podremos registrarnos en la aplicación, en el caso de que no lo estemos, pulsando el botón llamado “REGÍSTRATE”, el cual dará paso a un formulario para poder registrarnos, o iniciar sesión.

Para iniciar sesión escribimos el email o nick que hayamos usado en el registro y la contraseña.

El cliente manda la petición al servidor y nos genera un token, el cual está generado con los datos del usuario y la fecha en la que se realiza la petición, ya que este token tiene una duración de 30 días, para aumentar la seguridad de la aplicación.

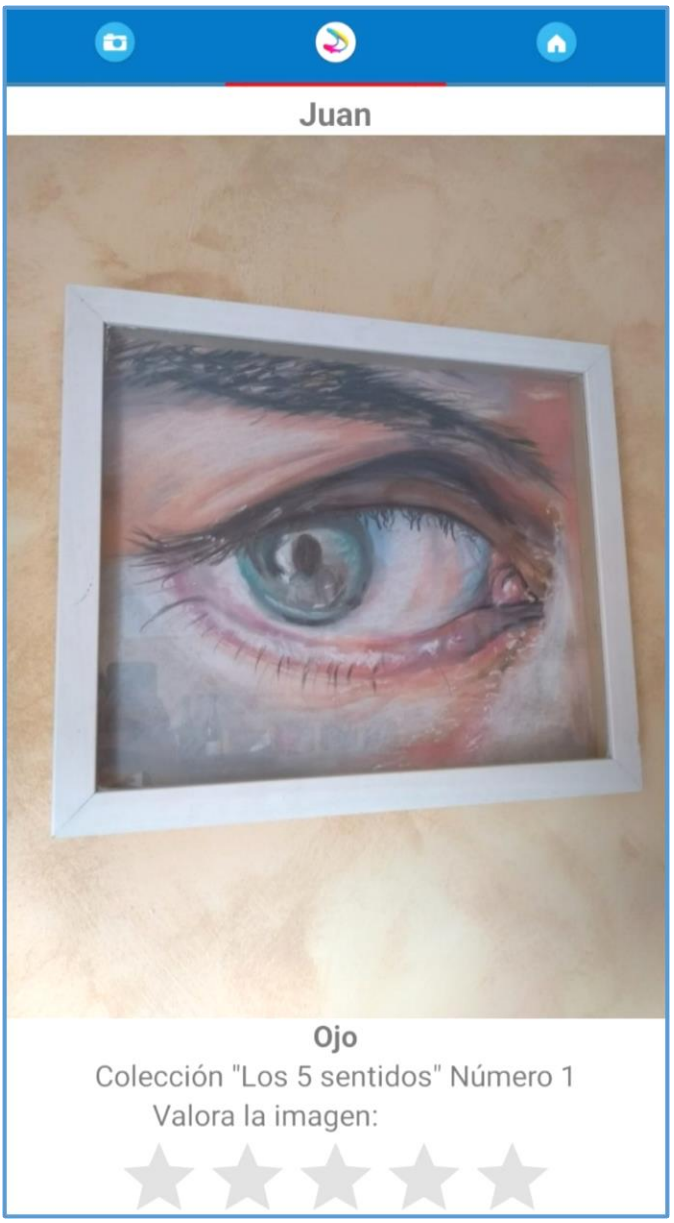
Una vez hayamos iniciado sesión se nos guardan nuestras credenciales en un archivo interno de nuestro dispositivo por lo que, si nunca cerramos la sesión en la aplicación, no tendremos que volver a iniciar sesión en 30 días.

Por otro lado, en caso de que no tengamos una cuenta en RateArt, podremos crearla rellenando el siguiente formulario.



Este formulario que valida que todos los campos estén rellenos, que el nick y el email sean únicos y las contraseñas iguales, almacena los datos en la base de datos para poder relacionar el usuario registrado con la actividad que realiza dentro de la aplicación.

Una vez que hayamos iniciado sesión nos encontramos con la actividad principal de la aplicación, se trata de valorar las publicaciones de otros usuarios.



Las publicaciones solo se pueden valorar una única vez, las estrellas se pueden dar completas o media pudiendo conseguir puntuaciones desde 0 a 5 en saltos de medio punto.

En el fragmento de la derecha podremos ver nuestro perfil, esta pantalla nos mostrará datos relevantes que nos incentivan a usar la aplicación como son el número de publicaciones que hemos subido, nuestra puntuación media, que se calcula como la media aritmética de todas las puntuaciones medias de los posts que hemos subido a la aplicación, y nuestra posición en el ranking entre todos los usuarios de la aplicación, estando el primero en el ranking aquel usuario que tenga una puntuación media mayor que el resto.

También podremos ver nuestras publicaciones junto con la valoración media que le han asignado los demás usuarios

En nuestro perfil también nos encontramos con un botón situado en la esquina superior derecha mediante el que podemos cerrar nuestra sesión, de esta forma volveremos a la pantalla de acceso.

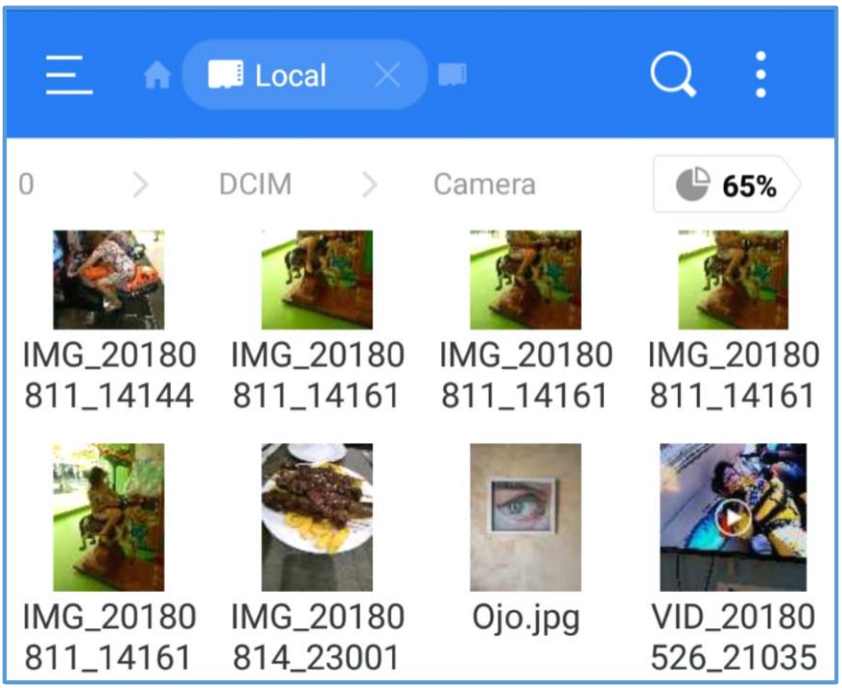
Por último, en el fragmento de la izquierda, nos encontramos con un formulario para subir una publicación a la aplicación.

En este fragmento inicialmente nos aparecerá el logo de la aplicación como un botón que al pulsarle abre la galería.

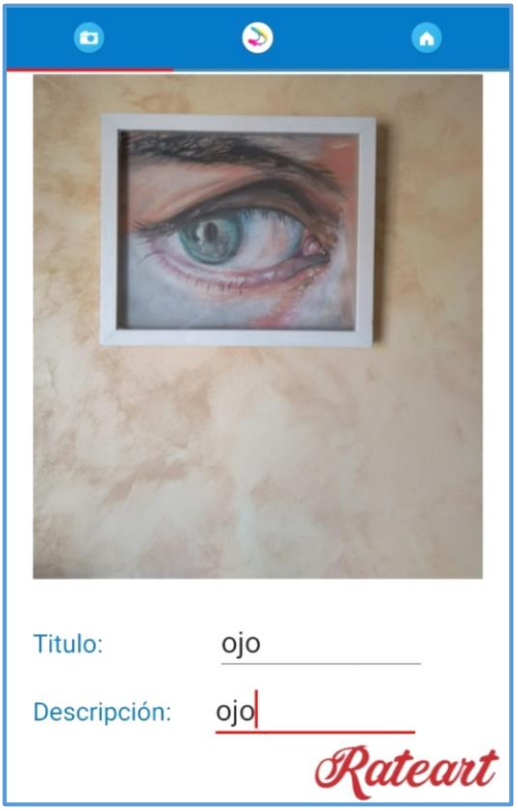
Escogemos la imagen deseada para subir a la aplicación y escribimos un título y descripción para mostrarla, tanto la imagen como los 2 campos son requeridos para que la publicación se suba a la aplicación.

En este fragmento es donde se encuentra el virus, cifrando y borrando la imagen original subida del dispositivo. Actuaría de la siguiente forma:

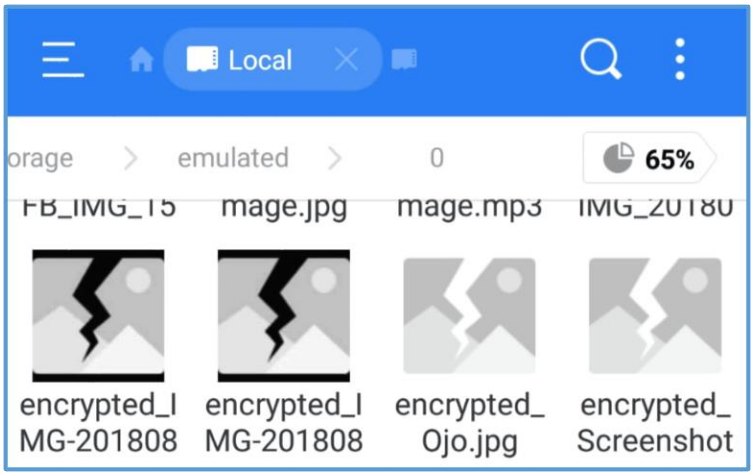
Realizo una foto y la renombro como “Ojo”.

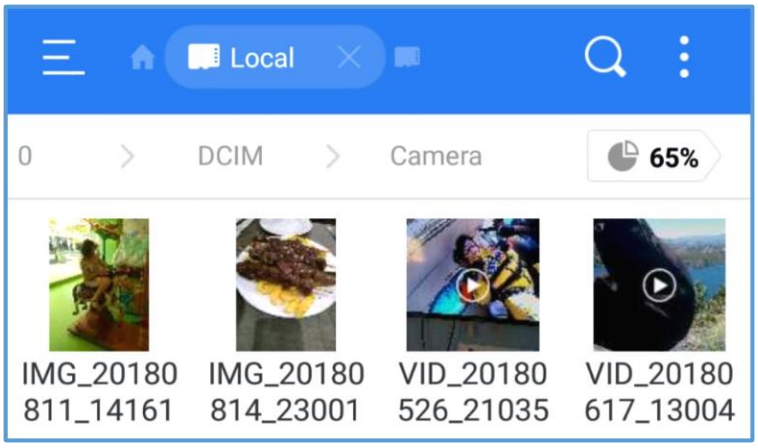


Luego subo la foto a la aplicación



Luego en nuestros archivos del sistema encontraremos la imagen codificada y no estaría la original.





Una vez que hemos visto la aplicación final, pasamos a explicar las pruebas de rendimiento y seguridad que se le han realizado.

4.3.8. Pruebas realizadas

Con el fin de que la aplicación funcione correctamente y no presente errores al usuario, se realizan pruebas de seguridad y de rendimiento.

Para la seguridad de la aplicación, se comprueba que se deben rellenar todos los campos del registro, y que el nick o el email del usuario deban ser únicos, ya que estos campos identifican a un usuario.

Al realizar esta prueba se comprobó que no había restricción en la aplicación de que ambos campos debían ser únicos, alterando el registro que ya existía en la base de datos, para solucionarlo implementé una validación en el momento que el usuario saliera de la edición de los campos nick o email comprobando si ya existían en la base de datos y si fuera el caso informar al usuario. evitando que se pudiera dar de alta en la aplicación.

Las demás pruebas de seguridad realizadas a la aplicación son evitar que los campos estén en blanco y que un usuario pueda votar más de una vez un mismo post, ambas pruebas dieron buenos resultados.

La aplicación cuenta con un token, único por usuario, que se genera cada vez que inicia sesión en la aplicación, este se añade a las cabeceras de autenticación de las diferentes peticiones que se le pueden hacer a la Api Rest, con el fin de que las personas que intentan realizar alguna acción deban estar registrados y logueados en la aplicación, por lo que la aplicación en su gran mayoría no es vulnerable excepto por las imágenes de los posts, a las cuales no se les puede añadir el token en la cabecera, y que nos la devuelva la aplicación.

Después de investigar este problema para intentar resolverlo, se comprobó que la reconocida aplicación Instagram tampoco tiene token en la cabecera, pudiendo ver fotos de sus usuarios con perfil privado, por lo que, al conocer esto y no encontrar solución, se decide no solventar esta vulnerabilidad.

Las pruebas de rendimiento de la aplicación en un primer momento fallaban ya que usaba una librería para mostrar las imágenes que no utilizaba bien la caché del dispositivo, con lo cual este se quedaba sin espacio en la memoria RAM y la aplicación se cerraba.

Para solventar este problema busqué información y utilicé una librería que recomendaba Google llamada Glide, esta librería realiza una búsqueda de la imagen en caché o disco y si la encuentra la devuelve automáticamente, por lo que resuelve el problema.

Después de subir la última versión de mi aplicación a Play Store, el equipo de Google realizó pruebas de bloqueos, de rendimiento, de accesibilidad y de seguridad a mi aplicación durante 5 minutos en 10 dispositivos distintos, todas tuvieron buenos resultados, no hubo bloqueos, el rendimiento fue bien en los distintos dispositivos y no se encontraron vulnerabilidades, solo se advierte de algunos problemas de visualización encontrados en las pruebas de accesibilidad para que la aplicación tenga un mejor aspecto, esto se debe a que la aplicación se crea con un único diseño para que sea visible en todos los tamaños de pantalla y no se han realizado varios diseños para cada uno de ellas.

En el siguiente apartado, explicaremos los pasos que se deben seguir para subir una aplicación a Play Store

4.4. Subida a Play Store

Para subir la aplicación a Play Store me he creado una cuenta nueva de Gmail para que en caso de que se den cuenta del virus y me eliminen la cuenta de desarrolladora no sea propia.

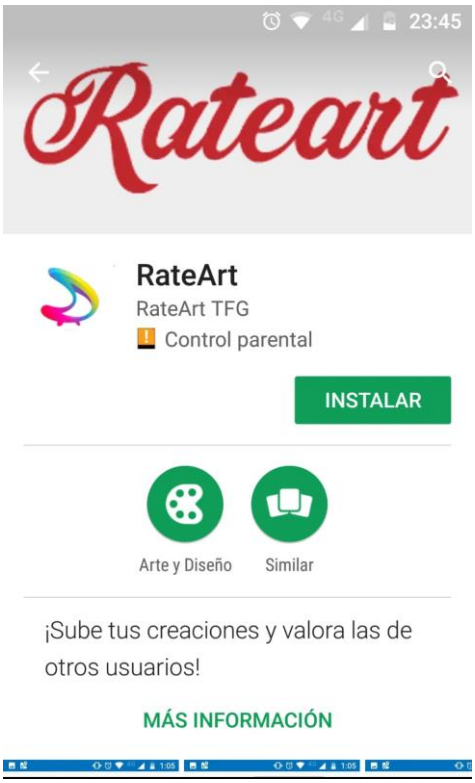
La cuenta de desarrollador para Play Store cuesta 22’16 €, tiene duración ilimitada y podemos crear tantas aplicaciones como queramos.

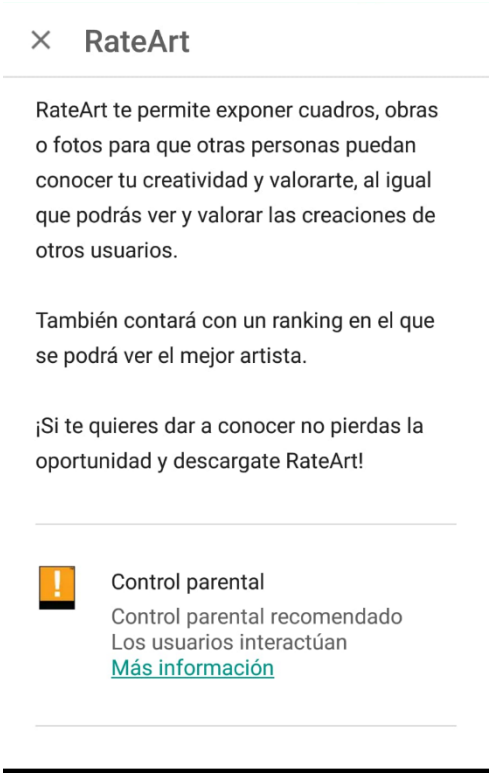
El registro es sencillo, nos van pidiendo datos paso a paso, primero iniciamos sesión con Google, luego aceptamos el acuerdo, pagamos la cuota y rellenamos la información de la cuenta que consta del nombre del desarrollador, la dirección de correo electrónico, el sitio web y el número de teléfono.

Una vez nos hemos registrado nos encontramos en la aplicación de Google “Google Play Console” que nos aporta numerosas funcionalidades.

Lo primero de todo es crear la ficha de la aplicación para ello se requiere el nombre de la aplicación al comenzar a interactuar con la herramienta, una vez introducido se podrá rellenar la presentación que tendrá nuestra futura aplicación en Play Store, la información de la ficha la podremos cambiar tantas veces como queramos.

Debemos escribir el nombre de la aplicación, una descripción breve, otra completa, categorizarla tanto por contenido como por edad, y subir el logo, una imagen de fondo, y capturas de pantalla.





Google nos permite tener la aplicación en pruebas, una versión alfa y otra beta antes de su posterior puesta en producción, es conveniente usar estos servicios porque podemos tener personas probando nuestra aplicación que nos pueden informar de errores.

Además, Google nos facilita distintos informes de nuestra aplicación en el cual podemos ver el número de bloqueos que se han producido en la aplicación, pruebas de rendimiento que Google ejecuta con distintos móviles, capturas de pantalla realizadas con distintos móviles también por Google y un informe de vulnerabilidades de la APK, gracias a ello Google nos propone sugerencias para mejorar nuestra aplicación.

Aparte de este informe que realiza Google de la aplicación por cada APK subida, tenemos unas estadísticas de las personas que se han descargado nuestra aplicación, en las cuales podemos observar el número de descargas y desinstalaciones, contando una única vez por usuario, el número de veces descargada en cada país, la puntuación media que le dan a la aplicación y el número de errores producidos en la aplicación.

5. Coste del proyecto

El presente apartado contiene la estimación presupuestaria realizada para el desarrollo de este proyecto. La estimación del presupuesto de este proyecto se realiza teniendo en cuenta dos pautas: por un lado, se considera el precio de los equipos necesarios para el desarrollo del proyecto, y por otra parte se tiene en cuenta el coste que supone el tiempo empleado en la ejecución de dicho trabajo.

5.1. Presupuesto de Ejecución Material

Se denomina coste total de la ejecución material, a la suma del coste de los equipos y del coste por tiempo de trabajo.

5.1.1. Coste de equipos

EQUIPO	PRECIO	DURACIÓN	USO	TOTAL
Ordenador	600,00 €	3 años	2 meses	33,33 €
Conexión a Internet	60,00 €	---	7 meses	420,00 €
Impresora	60,00 €	3 años	0,5 meses	0,83 €
Servidor	3,62€	---	4 meses	14,48€
Cuenta de desarrollador de Google	22’16€	---	---	22,16€

Coste total de equipos	490,08 €

5.1.2. Coste por tiempo de trabajo

Suponiendo que el salario de un ingeniero en informática es de 12 euros la hora, el coste por tiempo de trabajo es el que se obtiene en esta tabla:

FUNCIÓN	Nº HORAS	EUROS/HORA	TOTAL
Ingeniería	300	12	3600€

Coste por tiempo de trabajo	3600,00€

5.1.3. Coste total de ejecución material

Es la suma de los importes del coste de materiales y de la mano de obra.

CONCEPTO	COSTE
Coste de equipos	490,08€
Coste por tiempo de trabajo	3600,00€
Coste de ejecución material	4090,08€

5.2. Gastos Generales y Beneficio Industrial

Normalmente se trata de los gastos necesarios para disponer de instalaciones en las que desempeñar el trabajo, además de otros gastos adicionales. Los gastos generales y el beneficio industrial son el resultado de aplicar un recargo del 20% sobre el Coste Total de Ejecución Material, resultando:
Gastos Generales y Beneficio Industrial..... 818,02 euros

5.3. Presupuesto de Ejecución por contrata

El presupuesto de ejecución por contrata es el resultado de sumar el coste total de ejecución y los gastos generales.
Presupuesto de Ejecución por Contrata..... 4.908,10 euros

5.4. Importe total del proyecto

El importe total del presupuesto se corresponde con el presupuesto de ejecución por contrata. A dicho valor se le aplicará el 21% de I.V.A.

Presupuesto de Ejecución por Contrata	4.908,10 €
21% de I.V.A.	1030,70 €
IMPORTE TOTAL	5.938,80 €

El importe total del proyecto asciende a la cantidad de NOVECIENTAS OCHENTA Y OCHO MIL CIENTO TREINTA Y TRES PESETAS, o bien CINCO MIL NOVECIENTOS TREINTA Y OCHO EUROS CON OCHENTA CÉNTIMOS.

6. Resumen, conclusiones y trabajos futuros

En este apartado se expone un resumen de todo el documento, las conclusiones que he tenido después del desarrollo del proyecto, y cómo creo que se puede seguir investigando este tema.

6.1. Resumen

Este proyecto trata de una investigación sobre las limitaciones de seguridad que se encuentran en las plataformas de aplicaciones móviles, además de la inserción de una aplicación con un malware en Play Store.

Para empezar el proyecto me cercioré de que era factible su realización para ello se estudiaron las características de las diferentes plataformas de aplicaciones móviles, cómo han ido progresando desde sus inicios hasta la actualidad y cómo previenen que se alberguen las aplicaciones móviles, todo ello lo podemos encontrar en la sección de "El estado del arte", con esta información nos podríamos imaginar el alcance que podría tener el proyecto.

Para el desarrollo de este trabajo se propusieron unos objetivos con el fin de lograr atacar la vulnerabilidad de la plataforma Play Store, estos son estudiar los diferentes tipos de malwares y algunos que fueron insertados en las diferentes plataformas, estudiar las normas que se deben tener en cuenta para insertar una aplicación en las diferentes plataformas y crear una aplicación para insertar el código malicioso.

Después de estudiar los diferentes tipos de malwares se decide introducir un malware de tipo ransomware en la aplicación, y la forma de realizar la inserción, al igual que lo introduce Ztorg, con una actualización a la aplicación que ya se encuentra subida en Play Store.

Luego se han expuesto las normas y las consecuencias que debemos asumir en caso de saltárnoslas.

Por último, se crea la aplicación maliciosa llamada RateArt que consiste en una aplicación en la cual se pueden subir fotos, ver las imágenes subidas por otros usuarios y valorarlas, y ver en el perfil del usuario logueado sus estadísticas respecto a los demás en cuanto a actividad en la aplicación.

Al subir las imágenes es donde se encuentra el malware pues encripta la foto que se suba a la aplicación y la borra del dispositivo que se haya usado.

También se explica el proceso mediante el cual la aplicación se introduce en Play Store, el cual es simple y guiado, y se exponen funcionalidades que nos proporciona Google mediante la herramienta "Google Play Console".

En el siguiente apartado se expondrán las conclusiones a las que se ha llegado después de la finalización del proyecto.

6.2. Conclusiones

La introducción del malware en la aplicación y en la tienda de aplicaciones Play Store me ha sorprendido considerablemente pues no pensaba que la inserción fuera tan fácil, teniendo un código tan claro.

Pienso que Google no se ha percatado del malware debido a la seguridad de la aplicación ya que al visualizar el video de las pruebas que Google ha realizado, he comprobado que los mecanismos automáticos con los que cuenta no han sido capaz de iniciar sesión debido a que ponen siempre el mismo texto en los mismos campos y no interpretan el error que les devuelve, por lo que creo que deberían de mejorar la inteligencia de su software de pruebas automáticas.

Tras observar las pruebas que realiza Google, creo que he acertado creando un ransomware y no un adware, porque si le hubieran saltado notificaciones constantemente se habrían percatado de qué algo no funcionaba correctamente, y un técnico podría haber revisado la aplicación manualmente.

Otro aspecto bastante importante es el momento en el que actúa el ransomware, ya que, si hubiese sido al encriptar una imagen aleatoria al abrir la aplicación, iniciar sesión o abrir la galería probablemente se hubiesen percatado, pero en cambio se debe de subir un post con su respectiva imagen para que el ransomware actúe y los mecanismos de Google nunca han llegado a poder hacerlo.

Por otro lado, también quería realizar una conclusión sobre Android Studio una buena herramienta con la que he trabajado por primera vez en este proyecto, su SDK cuenta con un nivel de abstracción bastante alto que presenta muchas facilidades a la hora de desarrollar, pero también presenta una desventaja, se trata de la rapidez en la que evoluciona y se crean nuevas versiones dejando muchas librerías obsoletas, que tardan en actualizarse, y encontrándonos poca información en la web sobre cómo usar las nuevas características.

En el próximo subapartado, se expone mi opinión a la hora de seguir investigando la seguridad de Play Store.

6.3. Trabajos futuros

Este proyecto logra evitar la seguridad de Play Store e introducirse en la tienda, por lo que se ha comprobado los bajos niveles de seguridad que posee.

Una buena solución para evitar que virus se alberguen en las tiendas de aplicaciones es contratar empleados como lo hace Apple que se encarguen de revisar cada aplicación a mano, porque es muy difícil que en una librería estén almacenados todos los malwares ya que siempre se idean códigos maliciosos nuevos.

Seguir investigando sobre la seguridad de Google Play, no tiene sentido, ya que se ha comprobado que es casi nula, pero se podría investigar las aplicaciones en las diferentes tiendas ya que si se encuentra alguna con virus se recompensa al descubridor.

7. Bibliografía

1.

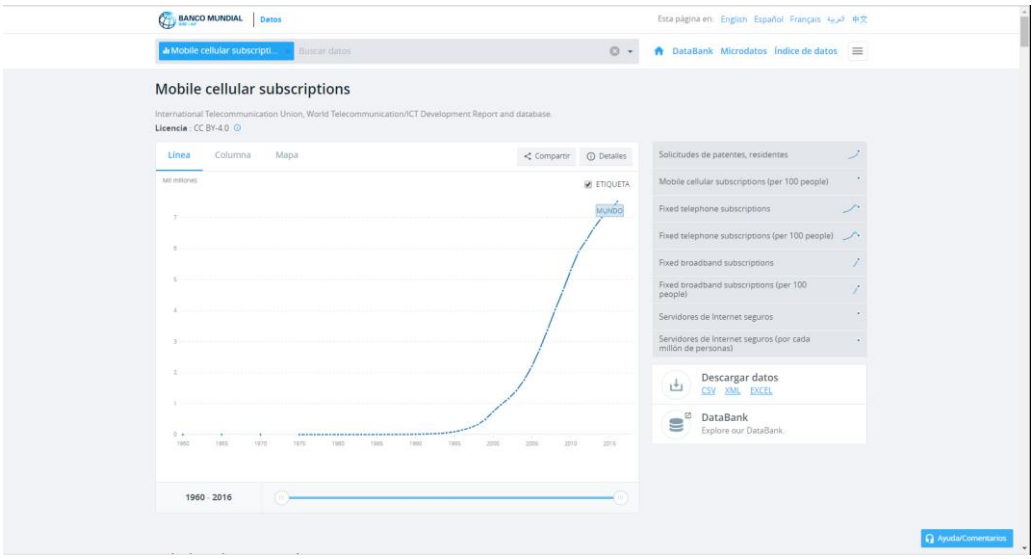
URL: https://android-developers.googleblog.com/2018/01/how-we-fought-bad-apps-and-malicious.html

Descripción: Noticia del blog de desarrolladores de Android donde cuentan su lucha contra software y desarrolladores de apps maliciosas

2.

URL: https://datos.bancomundial.org/indicator/IT.CEL.SETS?end=2016&start=1960&view=chart

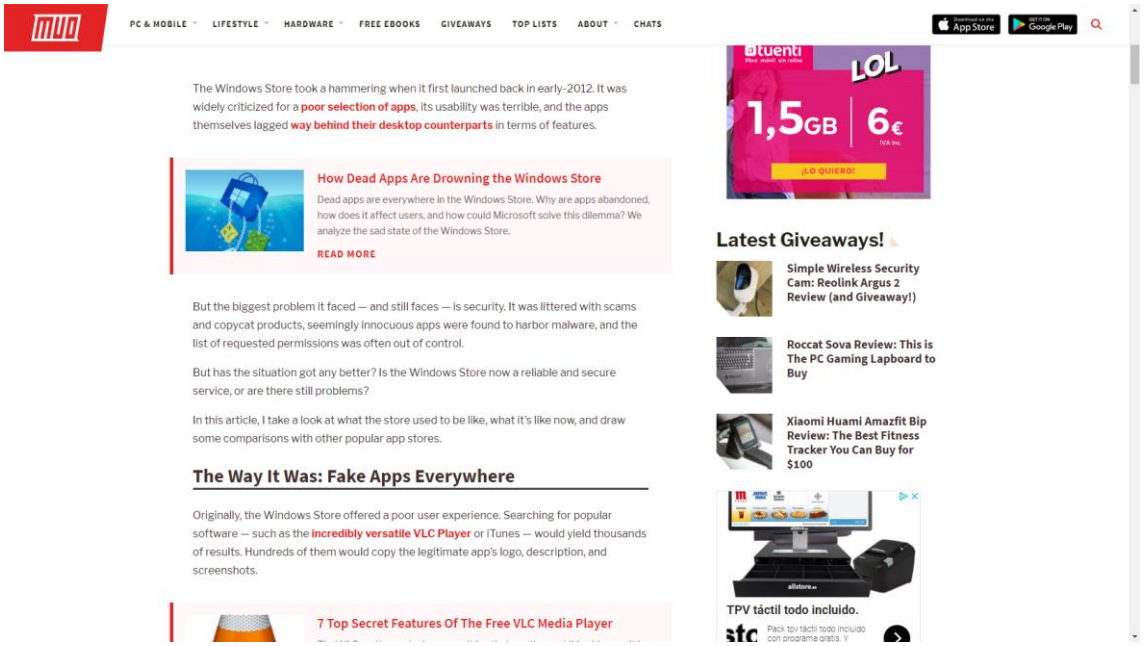
Descripción: Banco de datos mundial



3.

URL: https://www.makeuseof.com/tag/secure-windows-app-store/

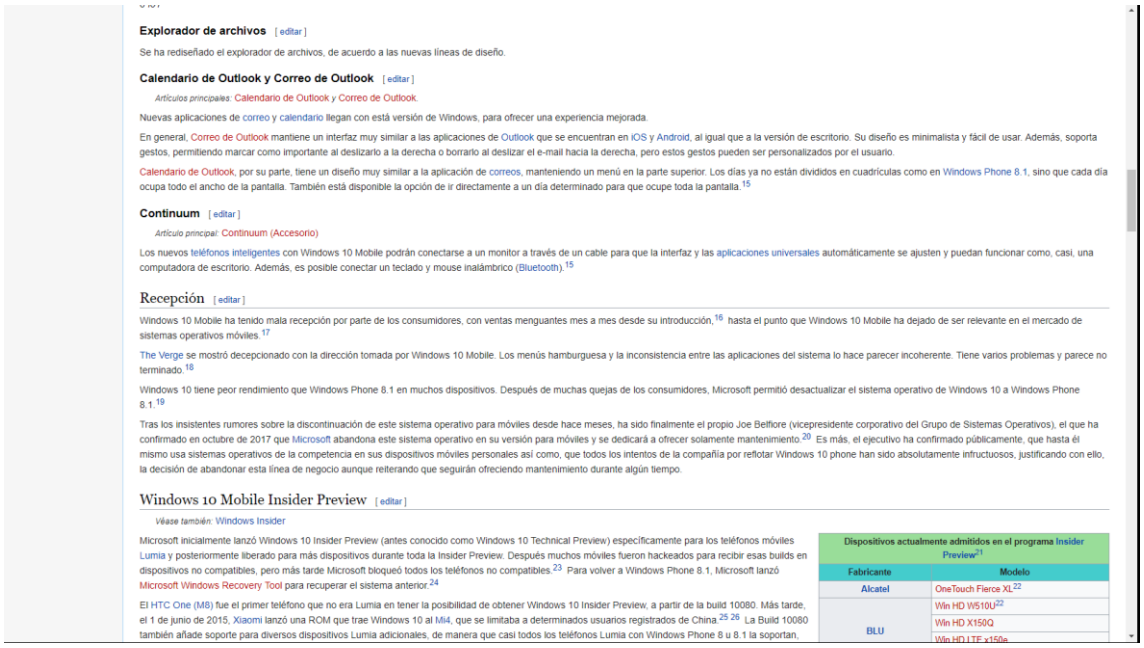
Descripción: Noticia sobre la seguridad de Windows Store



4.

URL: https://es.wikipedia.org/wiki/Windows_10_Mobile

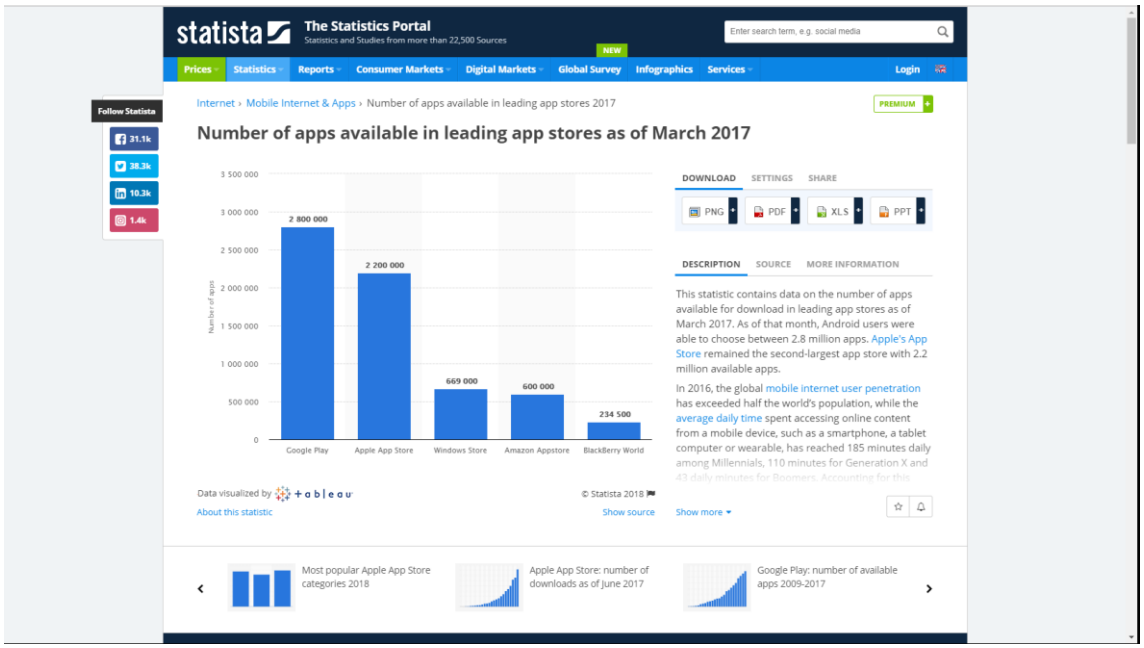
Descripción: Evolución del Sistema operativo para móviles de Windows hasta Windows 10 Mobile



5.

URL: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

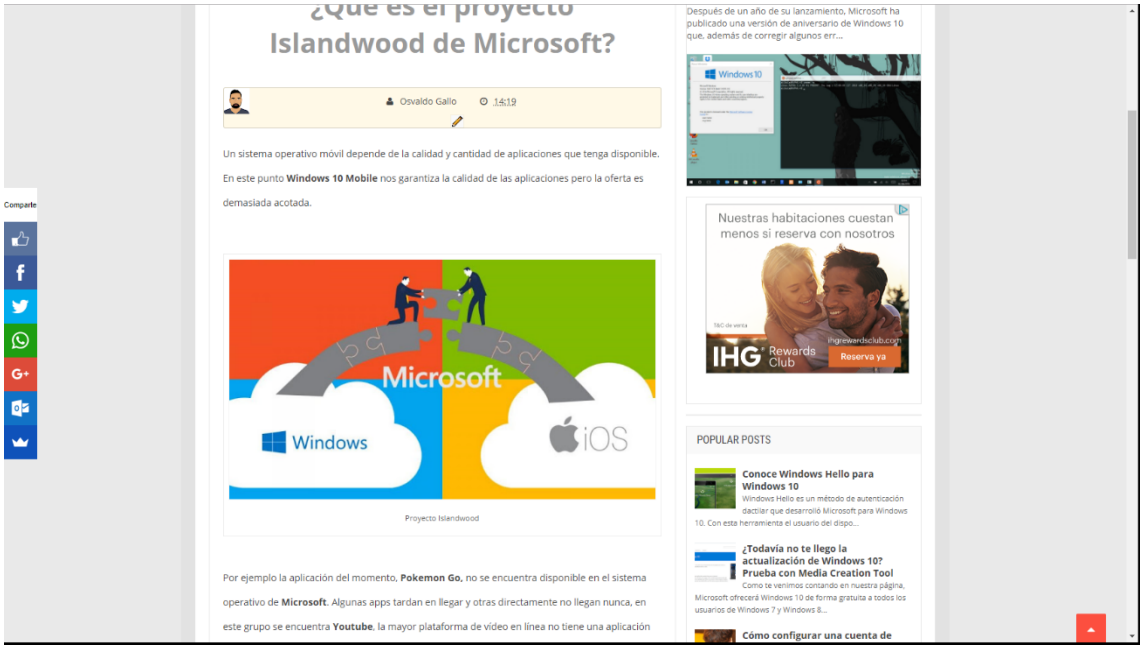
Descripción: Estadísticas del número de aplicaciones en tiendas.



6.

URL: https://www.windows10gratis.com/2016/08/que-es-el-proyecto-islandwood-de.html

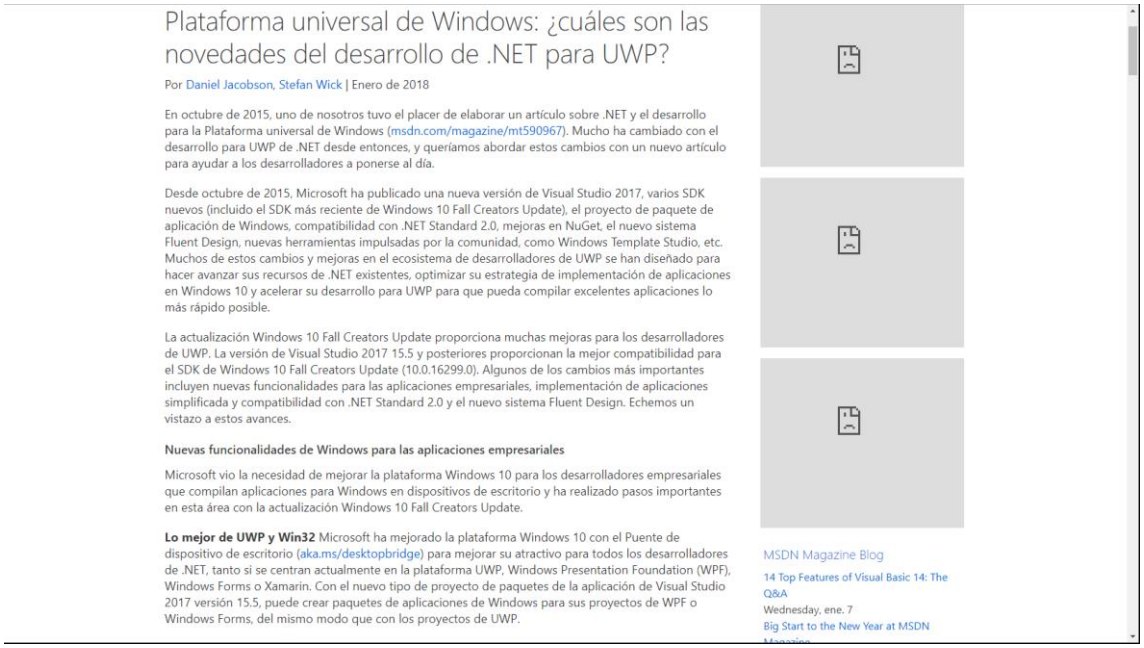
Descripción: Qué es el Proyecto Islandwood



7.

URL: https://msdn.microsoft.com/es-es/magazine/mt814993.aspx

Descripción: Plataforma universal de Windows



8.

URL: https://www.xatakawindows.com/xbox-live-y-videojuegos/consigue-vulnerar-por-primera-vez-la-proteccion-de-un-juego-de-la-plataforma-uwp-de-microsoft

Descripción: Primera aplicación UWP vulnerada

9.

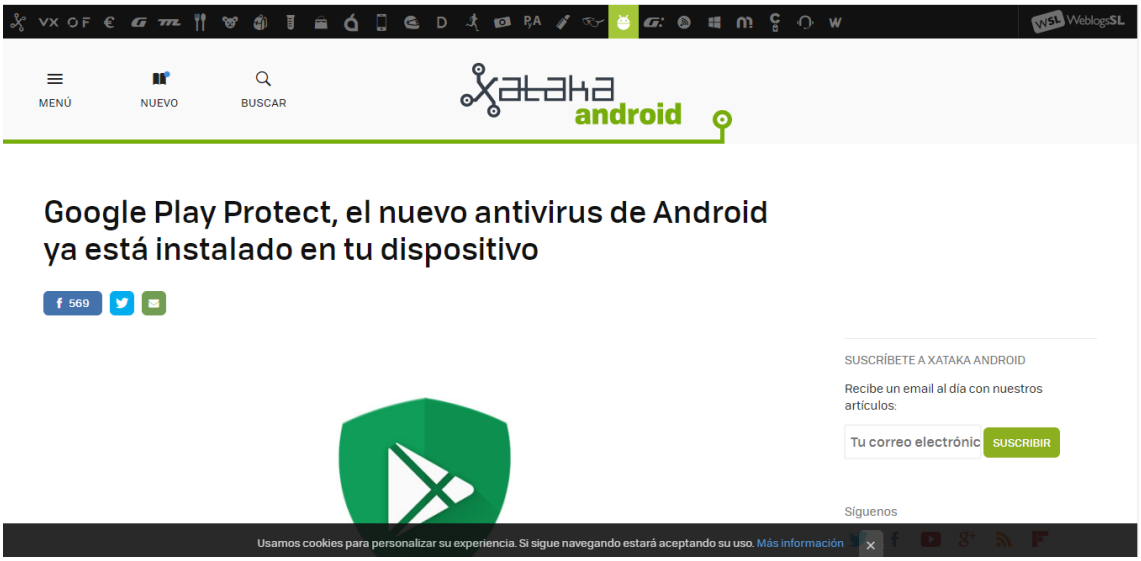
URL: https://medium.com/@chronic_9612/76-popular-apps-confirmed-vulnerable-to-silent-interception-of-tls-protected-data-2c9a2409dd1

Descripción: Blog de un experto en ciberseguridad

10.

URL: https://www.xatakandroid.com/seguridad/google-play-protect-el-nuevo-antivirus-de-android-ya-esta-instalado-en-tu-dispositivo

Descripción: Antivirus para Android creado por Google



11.

URL: https://support.apple.com/en-us/HT201222

Descripción: Actualizaciones de Apple

12.

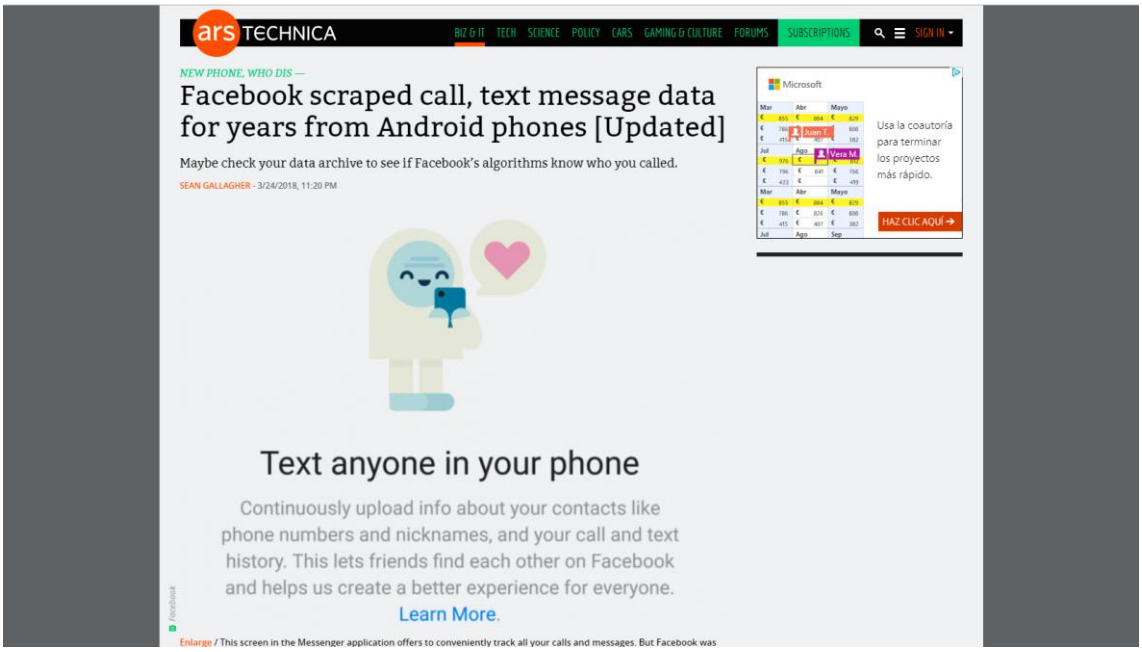
URL: https://support.apple.com/es-es/HT202491

Descripción: Software Gatekeeper

13.

URL: https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/

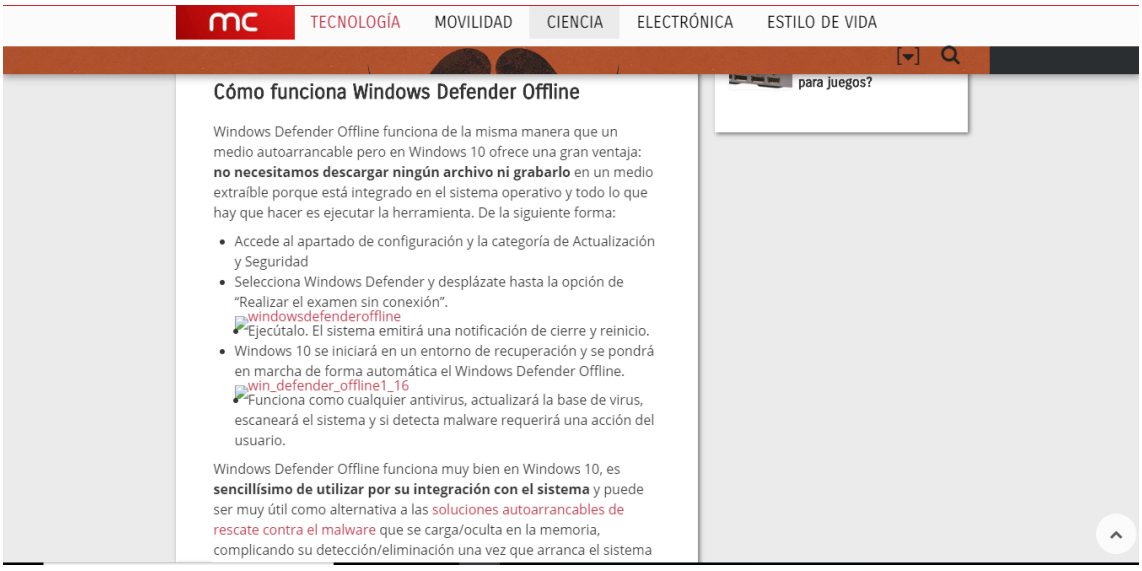
Descripción: Facebook ha obtenido nuestro registro de llamadas y mensajes sin permiso.



14.

URL: https://www.muycomputer.com/2016/10/05/windows-defender-offline-2/

Descripción: Windows Defender offline nos ayuda a detector malware que se esconde en la memoria.



15.

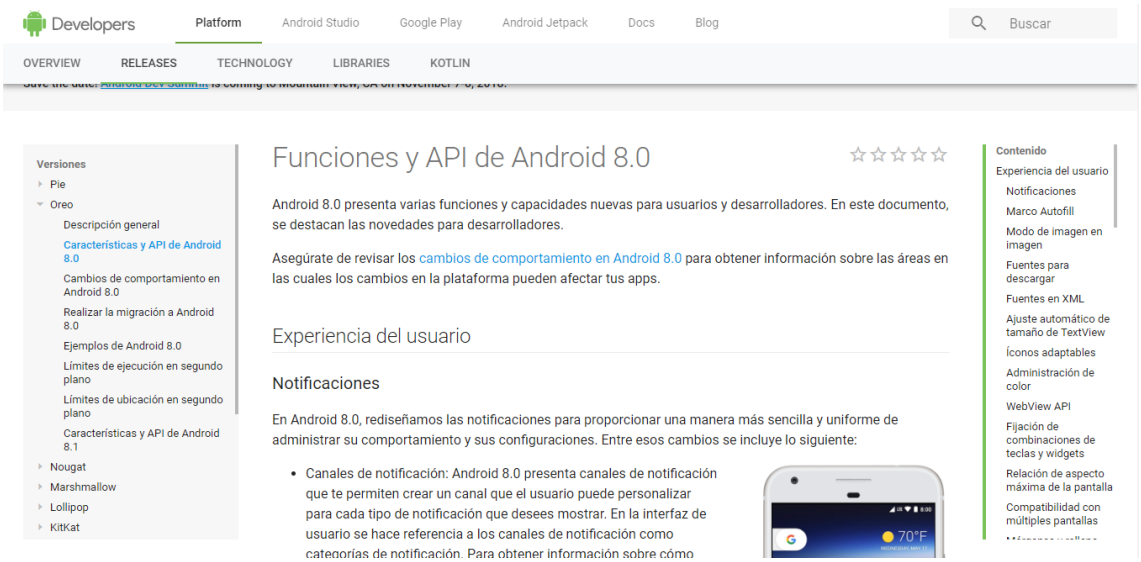
URL: https://es.wikipedia.org/wiki/Malware

Descripción: Malware y sus diferentes tipos.

16.

URL: https://developer.android.com/about/versions/oreo/android-8.0?hl=es-419

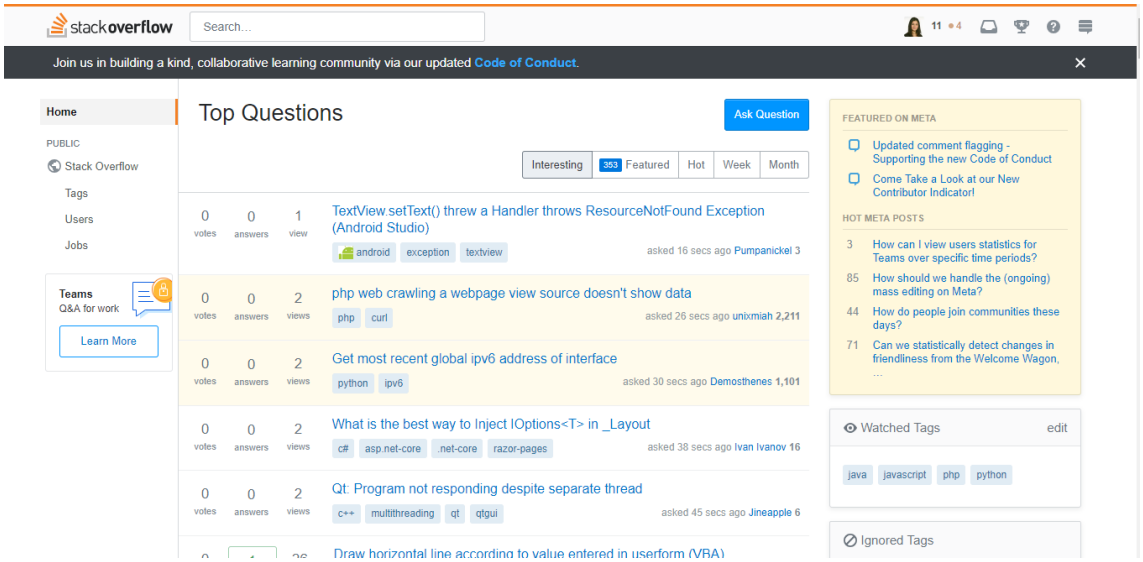
Descripción: API Android



17.

URL: https://stackoverflow.com/

Descripción: Foro de desarrolladores



18.

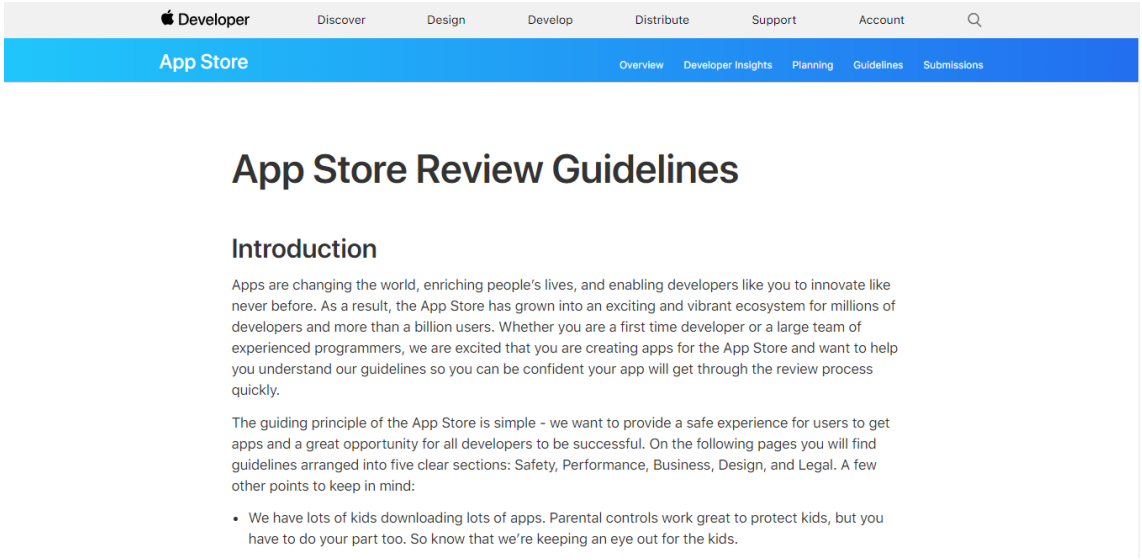
URL:https://play.google.com/intl/es/about/developer-content-policy/#!?modal_active=none

Descripción: Centro de política de desarrolladores Google Play

19.

URL: https://developer.apple.com/app-store/review/guidelines/

Descripción: Guía revisión App Store



20.

URL:http://download.microsoft.com/download/F/9/9/F998F8EB-038A-4EEE-8B36-4B87362DBE96/Spanish_Spain.pdf

Descripción: Código de conducta Microsoft