Resumen Analítica Especializado -RAE

Fecha de Realización:	22/08/2020
Programa:	ESPECIALIZACION DE SEGURIDAD INFORMATICA
Línea de Investigación:	Infraestructura Tecnológica y Seguridad en redes
Título:	SEGURIDAD EN DISPOSITIVOS MOVILES CON SISTEMA OPERATIVO ANDROID VERSION LOLLIPOP
Autor(es):	Cárdenas Garzón Lida Jazmin
Palabras Claves:	Sistema Operativo, Ataques, Riesgos, vulnerabilidades.
Descripción:	

En la actualidad el constante cambio y avances tecnológicos permiten usar dicha tecnología para labores cotidianas tanto personales como laborales, en éste caso hablando de los dispositivos móviles con sistema operativo Android desde su version Lollipop hasta la version 10. Tales dispositivos de acuerdo a la información que pueden alojar en ellos o que se puede compartir, usar en diversas transacciones o ser tratada como se requiera dependiendo de las necesidades, pueden llevar a convertirlos en un objetivo de ataque dependiendo de la intención del hacker informático, lo que permite asumir la valides de indagar sobre la información que los usuarios alojan en los medios electrónicos usados por ellos y la pertinente seguridad que le otorgan a la misma.

Teniendo en cuenta lo anterior se llega al objetivo de consolidar la información, investigar e identificar los ataques, riesgos y vulnerabilidades a los que se encuentran expuestos dichos dispositivos con el sistema operativo mencionado, dando a conocer el análisis realizado a lo relacionado con esta versión de Android para dichos aparatos y así brindar una investigación adecuada para fomentar y animar a poner en práctica un correcto manejo de controles para la seguridad tanto del hardware como del software de dichos terminales y la información contenida en ellos.

Fuentes bibliográficas destacadas:

-BARRIO ANDRES, Moisés. Internet de las cosas. Editorial Reus. 2018

-ECONOMIA Y NEGOCIOS. En el país hay más hogares con celular que con acueducto [En línea]. Bogotá: El Tiempo.com. 2017., Disponible en https://www.eltiempo.com/economia/finanzas-personales/colombianos-tienen-mas-celulares-que-servicio-de-agua-68584

-GIUSTO, Denise, Balance semestral de la seguridad móvil [En línea]. Bogotá: Welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

-GOBIERNO EN LÍNEA. Las tecnologías emergentes serán fundamentales para combatir el cibercrimen en Latinoamérica [En línea]. Bogotá: Entérate. 2018., Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/w3-article-80353.html

-TECNOLOGÍA EMPRESARIAL. El Factor humano como amenaza interna a la seguridad de la información [En línea]. Managua: El Nuevo Diario. 2013., Disponible en:

https://www.elnuevodiario.com.ni/economia/300466-factor-humano-amenaza-interna-seguridad-informacio/
-TECNOSFERA. Colombianos tocan su celular 2 mil veces al día en estas actividades. [En línea]. Bogotá: El Tiempo.com. 2019., Disponible en: https://www.eltiempo.com/tecnosfera/dispositivos/encuesta-de-consumo-movil-en-colombia-2019-389702
-TORO SANCHEZ, Cristian Giovanny, VARGAS CARVAJAL, Jesús Alfredo y otro. Guía para validar el nivel de seguridad de los permisos y uso de recursos de una aplicación móvil bajo plataformas Android. Trabajo de grado. Bogotá D.C: Universidad Católica de Colombia, Facultad de Ingeniería, 2015. 72 p.

Contenido del documento:

El documento mencionado contiene información acerca de los ataques más comunes al Sistema Operativo Android, riesgos, amenazas y vulnerabilidades de seguridad en el Sistema Operativo Android, arquitectura de seguridad del mismo, clases de dispositivos que operan con éste sistema operativo, características de un celular inteligente o Smartphone, usos del celular, Android e Internet de las cosas, así como unas recomendaciones para intentar mantener a salvo la información contenida en éstos dispositivos.
Estos dispositivos son usados para tareas cotidianas tanto personales como laborales, se han vuelto necesarios y son utilizados por personas de diferentes rangos de edad en todo el mundo.

Teniendo en cuenta que en ellos se maneja todo tipo de información, se vuelven foco de numerosas amenazas, fallas, riesgos y vulnerabilidades, aprovechando que los usuarios no tienen el conocimiento o la experticia para reconocer si están en riesgo o no, o simplemente no se percatan de las amenazas que los rodean, esto evidencia la necesidad de profundizar en dichos ataques, consolidando la información recopilada y dándola a conocer, para que los usuarios finales tengan mayor conocimiento y por ende busquen la manera de implementar mayores controles de seguridad, mitigando y contrarrestando dichos riesgos y así logrando de alguna manera poner un alto a los ciberdelincuentes.

La seguridad se divide en dos tipos, tal y como se observa a continuación:

La Seguridad lógica que se encarga de restringir y asegurar el software y la información que cada uno almacene, así como controlar quien accede a este y que manejo realiza, por ejemplo: se utilizan Controles de acceso, los cuales se encargan de la identificación y autenticación en el sistema, lo que permite prevenir el ingreso de personas no autorizadas.
Por otro lado se pueden definir roles, con ciertos permisos y modalidades de acceso, indicando que se le permite al usuario realizar frente a la información, tales como (lectura, escritura, ejecución, borrado, creación y búsqueda), así como también se realiza una generación de claves para llevar a cabo una transacción con cierta seguridad.
También se ejecutan Limitaciones a los servicios, mediante restricciones según la aplicación o el administrador del sistema.

La seguridad física que se encarga de aplicar medidas para prevenir y controlar la información y proteger el hardware frente a una amenaza natural o una amenaza ocasionada por el hombre, como pueden ser los Desastres naturales tales como: Incendios que pueden ser provocados por manejos inadecuados de sustancias, de la parte electrónica o acumulación y filtración de líquidos o suciedad.
Así mismo se debe llevar a cabo una Seguridad del equipamiento, como por ejemplo: la temperatura adecuada y según el límite de humedad, la verificación de los conectores usados, como el cableado en cuanto a Interferencia por acción de campos eléctricos, el corte de cables y su correcto estado.

Dentro del uso de estas técnicas también se genera el uso inadecuado dado por el ser humano, ya sea de manera consciente o inconsciente, con o sin conocimientos, quien dependiendo de sus intenciones puede causar daños o robar información, generalmente sin que los afectados se percaten de dicha situación.

Entre los ataques más comunes uno de los más fáciles y usuales vistos por la mayoría de las personas es el uso de información personal en cuentas falsas, en las cuales se usan datos de una persona con fines ilícitos, en estas cuentas se usa información muy básica, la cual se puede obtener por diferentes medios, los más usados son las redes sociales, cuentas de correo, aplicaciones de mensajería instantánea etc. Debido a que en las redes sociales se puede configurar sus datos personales sin tener restricción alguna, este tipo de suplantación de identidad resulta ser muy convincente y difícil de detectar para otras personas.

Otro ataque de suplantación común en internet es el llamado “phishing”, este método consiste en enviar correos electrónicos en los cuales son usados nombres de empresas, personas, anuncios falsos entre otros, estos mensajes solicitan al usuario diligenciar sus datos para poder acceder a sus cuentas, verificar datos los cuales son muy confidenciales u obtener premios, algunos usuarios no reconocen estos mensajes falsos, dejando expuesta su información y resultan siendo víctimas de grandes estafas. Entre los diferentes ataques de suplantación de identidad uno de los más eficaces y rápidos es el “web spoofing “ este ataque consiste en enviar un link falso al usuario el cual lo re-direcciona a una página en común en la cual el usuario conoce y confía, ya estando vinculado en esta página el usuario puede usar sus servicios como si fuese la página real, pero al momento de redireccionar algún ingreso de cuenta el usuario es redireccionado a otra página al azar, para algunas personas es muy fácil saber que su información ha sido robada, otras piensan que fue un simple error y no toman las precauciones necesaria para evitar ser estafados, suplantados entre otras acciones que se puede realizar con su información privada.

Los delincuentes informáticos sacan provecho del valor e importancia que tienen estos activos para una empresa o persona y con ello pueden alterar, sustraer, modificar, dañar, robar o incluso secuestrar la información con el fin de obtener un beneficio ya sea económico, social o por satisfacción propia.
En algunas ocasiones se puede presentar que las personas cometan ciber-delitos, por el desconocimiento de las leyes y las normas o simplemente por el hecho de estar llevando a cabo experimentos que se desencadenan en dichas infracciones.
Con estos antecedentes es fácil detectar que los usuarios no dimensionan los riesgos, peligros y amenazas a los que constantemente están expuestos, generando de esta manera un camino bastante amplio para que los cibercriminales logren sus objetivos.

El sistema operativo Android, el cual muestra con las evoluciones de sus versiones y actualizaciones el constante interés por consentir al usuario final y concederle la mejor calidad en cuanto a servicios y funcionalidades se refiere, naturalmente que no deja de lado la firme convicción de procurar la mejor protección en cuanto a seguridad del dispositivo y de la información que el contiene, Android es el más usado en los dispositivos móviles, hablando de las actualizaciones de éste sistema operativo se muestra que los usuarios no van avanzando a la par con las actualizaciones o versiones lanzadas por el administrador del sistema operativo, dejando una posible brecha de seguridad.

Ahora pasando por la percepción de seguridad se revela que para los usuarios el celular es seguro y en la mayoría usan sistemas de autenticación que brindan cierta seguridad en cuanto a la información se refiere, aunque un porcentaje no muy bajo expone claves o contraseñas y posiblemente más datos confidenciales por medio de las apps que éstas tecnologías permiten emplear.

Marco Metodológico:

Se realiza la selección de un tema a tratar, delimitando dicho tema posteriormente; se lleva a cabo una recolección y recopilación de la información relacionada, la cual pasa por un proceso de análisis que finalmente conlleva a la elaboración de un informe para la respectiva muestra de los resultados obtenidos.

Para la captura de los datos que se pretenden recopilar con el fin de identificar la percepción e identificación de la seguridad en los usuarios del sistema operativo Android Lollipop y/o sus versiones posteriores, se procede a efectuar la encuesta que es una de las “estrategias más utilizadas en el área de investigación.

Conceptos adquiridos :

Existes más malware y/o ardware de los que se puedan imaginar, algunos tal vez poco mencionados, por ejemplo:

Hummingbad es un malware que básicamente logra descargar aplicaciones sin que el usuario se tome la molestia de autorizarlo a dar el permiso para que esto suceda.
Hiddad este troyano logrando una vez instalado lanzar múltiples anuncios publicitarios, hiddad en especial se hace pasar por una aplicación que mide el pulso cardiaco pero su finalidad es lanzar anuncios publicitarios.

Conclusiones:

A partir de la revisión bibliográfica se concluye que el componente humano tiene un papel importante en abrir o no las puertas a la inseguridad de los dispositivos con el S.O. Android, cuando las personas se concientizan de llevar a cabo buenas practicas, esto ayuda en la mitigación de las vulnerabilidades y riesgos a los que se está expuesto.

Dentro del estudio de seguridad en S.O. Android se puede concluir que un gran porcentaje de la población utiliza éste sistema operativo, empleando sus dispositivos para tareas personales y laborales, siempre es importante verificar la procedencia de las aplicaciones que se instalen y usen en los dispositivos, así como asegurarse de navegar en páginas seguras en la web y de no descargar archivos de fuentes sospechosas.

Después de analizar la información recopilada acerca del S.O. Android a nivel de seguridad se estimó que los usuarios lo perciben muy seguro y aun cuando en las tiendas oficiales de Android se esfuercen por garantizar la seguridad de las apps que se pueden encontrar allí, esto no asegura que todo lo encontrado en ésta sea cien por ciento seguro. Así mismo la seguridad informática no está completamente garantizada para un sistema operativo, bajo ningún medio y para ningún dispositivo, por lo tanto es importante la consulta en fuentes confiables del nivel de seguridad para lo que brindan las tecnologías.

Cabe señalar que las técnicas usadas en seguridad informática, así como pueden generar un ambiente y entorno satisfactorio, también pueden ser usadas de manera malintencionada dependiendo de la ética profesional y personal de las personas que la utilizan. Se debe estar preparado para todos los posibles usos que se le pueda dar a las ciencias y técnicas aplicadas en los ambientes informáticos y tecnológicos, para garantizar la seguridad de la información y de los medios que la salvaguardan.