Detección de amenazas informáticas de tipo Malware Bancario o Ransomware Móvil hacia dispositivos Android, integrando IOC en una técnica semiautomatizada y con base en comportamientos analizados de incidentes.

Oscar Darío Arango Gómez

Instituto Tecnológico Metropolitano

Faculta de Ingenierías

Medellín, Colombia

2022

Detección de amenazas informáticas de tipo Malware Bancario o Ransomware Móvil hacia dispositivos Android, integrando IOC en una técnica semiautomatizada y con base en comportamientos analizados de incidentes.

Oscar Darío Arango Gómez

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

Magister Héctor Fernando Vargas Montoya

Línea de Investigación:

Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2021

(Dedicado a mi Madre, Esposa, Hija, Nietas y CORNARE)

Se suele medir el éxito de las personas por las cosas materiales que logran adquirir durante su vida, pero el verdadero éxito nada tiene que ver con ello, si no con el amor de una familia, la estabilidad laboral, y la tranquilidad de haber logrado conseguir cada una de las metas con esfuerzo y dedicación.

Oscar Arango Gómez.

Agradecimientos

De las cosas más valiosas en la vida es ser agradecido, porque solo puedes lograr las cosas, pero te demoraras más, en cambio con ayuda de otros, acompañado y guiado de personas maravillosas que conoces en la vida lograras llegar más lejos.

Tengo un eterno agradecimiento a mi Querido Profesor Héctor Fernando Vargas, quien con su tranquilidad, paciencia, amor por lo que hace, guio cada uno de mis pasos en esta dura lucha por alcanzar el reconocimiento de Magister, a mis profesores quienes con su abnegada entrega de su conocimiento brindaron para mí, educación de calidad y excelencia, a mi amada institución ITM, a la que le guardo un profundo amor, pues en ella he tenido logros que me han hecho crecer en mi vida personal y profesional, a CORNARE por su apoyo incondicional en mi formación por el tiempo y paciencia para poder lograr un objetivo más en mi vida.

Resumen

En la Actualidad el uso de dispositivos móviles se ha arraigado de tal manera que dependemos y depositamos toda la información relevante en ellos, por lo anterior es de vital importancia asegurar y cuidar el activo más valioso, la información personal en estos dispositivos.

Algunas de las amenazas hacia los dispositivos móviles como los Smartphone se ve reflejado en ataques como el robo de información o el cifrado malicioso, ejecutado a través de malware de tipo Ransomware, por lo cual, para lograr proteger la información lo primero es determinar si un comportamiento es anormal dentro del dispositivo ya sea real o sospechoso o si se trata de un incidente de seguridad o no. Por lo anterior, en este proyecto de grado de maestría se hizo una identificación de amenazas (Ransomware) usando indicadores de compromiso IoC y proponiendo diferentes medidas de control para la reducción de posibles impactos negativos.

Por esta razón, el proyecto se desarrolló en varias fase, en la Fase 1 se realizara el estudio de las distribuciones de Android que se usaran ara el desarrollo de esta tesis, enfocándonos en el mayor uso, adicional fue necesario determinar el estado del sistema antes de la ocurrencia de un evento de seguridad para cuando se presente el evento, mediante la caracterización de los Malware bancarios para dispositivos móviles tipo Android en sus dos últimas versiones más usadas, y realizando la caracterización de estos malware por medio de los IoC y así poder comparar en línea la afectación de algún proceso del teléfono haciendo una revisión de múltiples variables como lo son aumento del tráfico de red, alto consumo de CPU o de memoria RAM, lentitud en la respuesta de procesos, ejecución de aplicaciones extrañas, cambios en los archivos de configuración, que en conjunto permiten detectar o inferir que algo extraño está ocurriendo y de forma paralela empezar a perfilar una respuesta acorde con la tipología del evento., después de verificar el estado del sistema se procede a caracterizar los diferentes Indicadores de compromiso para dispositivos móviles.

En la Fase 2 se determinó un Mecanismo de clasificación de acuerdo al nivel de impacto de las amenazas al dispositivo Móvil con lo cual se realiza una construcción propia de una tabla de clasificación.

En la Fase 3 se realizó la construcción de una herramienta semiautomatizada, que, con baja intervención del usuario, se pudo detectar, clasificar y proponer una remediación básica en tiempo real algunos tipos de malware que quiera afectar un dispositivo.

Seguidamente, se conoció la afectación que un Malware realiza en un dispositivo y para esto se tienen los Indicadores de Compromiso o IoC, los cuales describen de forma clara y precisa el actuar y afectación de diferentes códigos maliciosos, luego de tener identificado claramente el actuar de cada código malicioso, se procedió a cargar los IOC a la herramienta semiautomatizada, la cual basada en comportamientos de los procesos del Android en sus dos últimas versiones, se encargara automáticamente de contener la amenaza.

En la Fase 4 se realizó la validación del proceso de detección, clasificación y control, así se determinó si esta herramienta logra la protección dispositivos móviles que son usados para las labores diarias, con ello lograr una acción de protección activa y en línea que permita reducir en tiempo real posibles riesgos.

Palabras clave: Android, Ataques Informáticos, Incidente de Seguridad, IOC, Malware Bancario, Ransomware, Semiautomatizada, Smartphone.

Abstract

At present, the use of mobile devices has taken root in such a way that we depend on and deposit all the relevant information on them, therefore it is of vital importance to ensure and take care of the most valuable asset, the personal information on these devices.

Some of the threats to mobile devices such as Smartphones are reflected in attacks such as information theft or malicious encryption, executed through Ransomware-type malware, therefore, in order to protect information, the first thing is to determine if a behavior is abnormal within the device whether real or suspicious or whether it is a security incident or not. Therefore, in this master's degree project, an identification of threats (Ransomware) was made using IoC compromise indicators and proposing different control measures to reduce possible negative impacts.

For this reason, the project was developed in several phases, in Phase 1 the study of the Android distributions that will be used for the development of this thesis will be carried out, focusing on the greatest use, additionally it is necessary to determine the state of the system before of the occurrence of a security event for when the event occurs, through the characterization of banking malware for mobile devices such as Android in its last two most used versions, and characterizing these malware through IoCs and thus be able to compare online the affectation of some phone process by reviewing multiple variables such as increased network traffic, high CPU or RAM memory consumption, slow response of processes, execution of strange applications, changes in files of configuration, which together allow us to detect or infer that something strange is happening and in parallel begin to outline a response in accordance With the typology of the event, after verifying the status of the system, we proceed to characterize the different Compromise Indicators for mobile devices.

In Phase 2, it is intended to determine a classification mechanism according to the level of impact of the threats to the mobile device, with which an own construction of a classification table is carried out.

In Phase 3, the construction of a semi-automated tool will be carried out, which, with low user intervention, detects, classifies and remediates in real time some types of malware that wants to affect a device.

Next, it is necessary to know the affectation that a Malware carries out on a device and for this we have the Indicators of Compromise or IoC, which clearly and precisely describe the action and affectation of different malicious codes, after having clearly identified the act of

each malicious code, we will proceed to upload the IOCs to the semi-automated tool, which, based on the behavior of the Android processes in its last two versions, will automatically take care of containing the threat.
In Phase 4, the validation of the detection, classification and control process will be carried out, in this way it will be determined if this tool achieves the protection of mobile devices that are used for daily tasks, thereby achieving an active and online protection action that allows reducing possible risks in real time.

Keywords: Android, Computer Attacks, Security Incident, IOC, Banking Malware, Ransomware, Semi-automated, Smartphone.

Contenido

Lista de figuras

Pág.

Lista de tablas

Pág.

Introducción

[53]Los dispositivos móviles se caracterizan por ser un sistema de comunicación ampliamente difundido debido a su fácil acceso, conectividad y versatilidad, cuentan con sistemas operativos similares a un computador, y tienen la ventaja del uso de redes geográficamente distribuidas a nivel global, lo cual los hace vulnerables a riesgos derivados por malware o ataques informáticos. Para el 2020 De acuerdo a los datos ofrecidos por Yi Min Shum, en el 2020 había 5.190 millones de usuarios únicos en dispositivos móviles, de los cuáles un 74% utilizan el sistema operativo Android, mientras que el otro 25% usan iOS [50].

Debido a la gran importancia y uso de los dispositivos móviles en la humanidad tanto en el ámbito personal como empresarial, se presenta una problemática en materia de seguridad que exhibe el uso de estos debido al crecimiento y aparición de malware constantemente, queriendo robar información dada la importancia adquirida y los datos ahí guardados [1].

En ese sentido surgen algunas cuestiones por definir, en primer lugar, el ¿cómo evitar que los usuarios utilicen el dispositivo con fines que no sean los corporativos?, en segundo lugar, se plantea la necesidad de identificar los riesgos presentes en el uso y almacenamiento de información sensible en las memorias de almacenamiento de los dispositivos móviles (como las MicroSD). Partiendo de lo anterior se determina que las principales debilidades de seguridad en el uso de estos elementos, son inherentes a la tecnología, las aplicaciones y al factor humano.

[2] En un estudio realizado por múltiples compañías, se señala que actualmente "*los dispositivos móviles contienen una gran cantidad de información confidencial de sus propietarios, convirtiéndose en un importante elemento para ellos y transformándose en una extensión de sus propias identidades*.", razón por la cual se examina la seguridad en dichos dispositivos, basados en el análisis de los hábitos y riesgos de los usuarios de móviles, tabletas y computadores portátiles, pero es una solución técnica que controla las posibles infecciones dejando un poco por fuera recomendaciones generales.

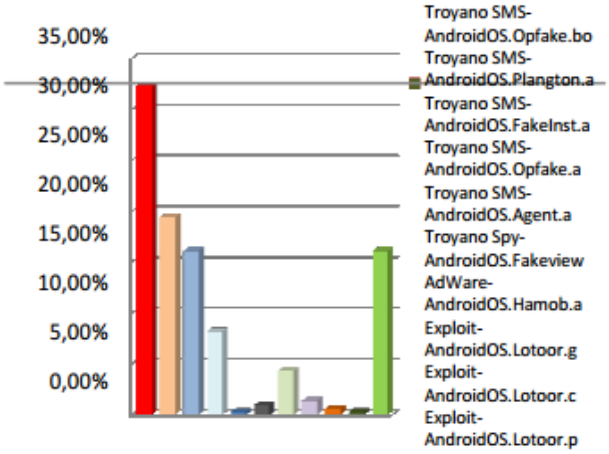
Existen algunos IoC para la interacción con diferentes Malware, pero no es clara la existencia de una aplicación proactiva o en línea que haga uso de estos en los dispositivos móviles, se puede encontrar bibliografía hablando de los IoC como estudio de patrones de los ciberataques más comunes y describiendo muy bien su funcionamiento, nivel de compromiso en los ataques, pero no existe en el medio un desarrollo de una aplicación móvil experta en la ejecución en línea de los IoC detectando y neutralizando un ataque cuando ocurra este.

[4] En muchos informes se menciona que no hace muchos años los dispositivos móviles se encontraban casi exentos de varios riesgos de seguridad al no estar interconectados con la red; pero que con los avances tecnológicos que permiten a dichos dispositivos conectarse y descargar contenido de la red, actualmente se encuentran expuestos a las

mismas amenazas de seguridad que los equipos informáticos. Un antecedente importante por lo cual se deben proteger los móviles de forma acertada y en tiempo real fue el caso Stagefright, un ataque que podía infectar a todos los Android y que no requería que el usuario hiciera nada. Simplemente, con recibir un mensaje multimedia, el equipo quedaba a merced del atacante. El informe sobre amenazas móviles afirma que "*los dispositivos móviles son la tecnología de consumo de más rápido crecimiento*", además, señalan que las aplicaciones móviles están convirtiendo a estos dispositivos en una plataforma de computación de uso general y que, como su popularidad van en aumento, también lo hacen los incentivos para los atacantes. Por lo anterior, analizan diferentes amenazas que afectan principalmente a las plataformas iOS y Android, por lo cual, tener un sistemas o mecanismos de visualizar esas amenazas e indicar a los usuarios como afrontarlas es un reto.

[17] Con la llegada del nuevo servicio en la nube KSN de la compañía Kaspersky Lab diseñado para prestar servicio a los dispositivos móviles con plataforma Android, se facilitó la recopilación de información y estadísticas, que permitieron determinar las amenazas detectadas con mayor frecuencia en dichos dispositivos como se muestra en la figura 1:

La figura 1. muestra los principales ataques contra el sistema operativo Android donde se evidencia los troyanos. Fuente: tomada de KSN Kaspersky



Por lo anterior, es importante ahondar en el conocimiento de los IoC (Indicadores de Compromiso) pero aplicándolo a los dispositivos móviles (Smartphone) y adicional crear una herramienta que automatice los controles a los riesgos. Por otro lado, las firmas simples de los IDS e IPS son demasiado fáciles para un intruso para ser eludidos, además estos no contemplan firmas importantes para el tema de Malware y tampoco instalar un IDS en Android. Las organizaciones deben ser capaces de comunicar cómo encontrar atacantes en sus redes y hosts, usando un formato digerible de la máquina que elimine el retraso humano asociado al intercambio de inteligencia, esta debe ser en el momento exacto que ocurren los eventos y con ello poder tomar acciones activas que reduzcan los riesgos y posibles amenazas [5].

Por otro lado, España [6] es uno de los países de habla hispana donde más se han realizado estudios y desarrollos basados en los indicadores de compromiso, como lo es el centro criptológico nacional del Gobierno Español, quien analiza mediante técnicas de indicadores de compromiso y reglas YARA, códigos maliciosos. Dichos informes los podemos encontrar en su página Web oficial, https://www.ccn.cni.es/ donde se analizan diferentes ciberataques y códigos maliciosos que afectan los sistemas de información y realizan un completo informe de la actividad sospechosa, incluyendo en esta los IoC y reglas YARA para su detección y ayuda en el análisis forense.

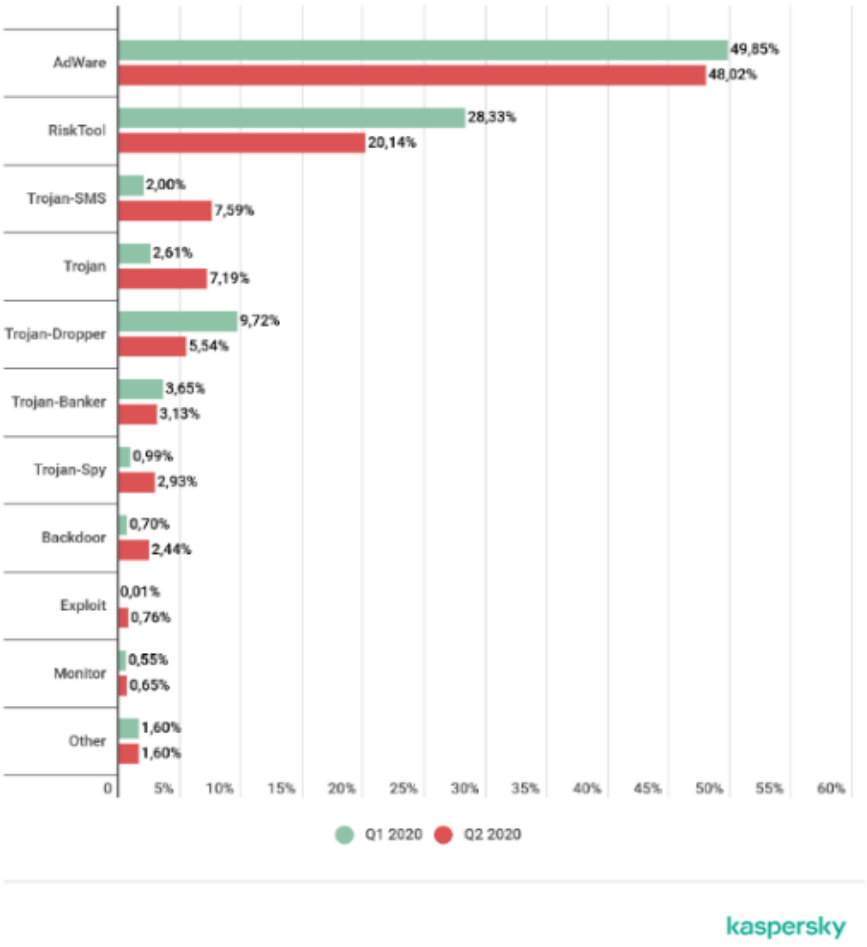
[34] las técnicas de detección de los IOC, son aplicados en los modelos que actualmente existen y que de una u otra forma ayudan en la mitigación de riesgos de seguridad informática estos también están enfocados en diversas plataformas como lo son Windows, Linux, DNS, plataformas de aplicaciones, pero realmente no se han enfocado en los dispositivos móviles, porque aún no se le ha dado la importancia que merecen por esto, esté caso de estudio da aplicabilidad e innovación en la automatización de un agente APK semiautomatizado para Android que aplique Indicadores de compromiso en los dispositivos móviles Android basado en reglas YARA e indicadores de compromiso.

La minimización de la ventana de exposición entre el tiempo de detección de un incidente y su respuesta, es un factor clave en el proceso de respuesta a incidentes, debido a la gran cantidad de información que se requiere para esta detección y la generación de conclusiones o inferencias que den paso a acciones de contención, corrección y recuperación, que es lo que debe aplicar un CSIRT es necesario un procedimiento automatizado que facilite la identificación de incidentes ya analizados y permita compartir dichos hallazgos con la comunidad para una actuación global. Como respuesta a esta necesidad han surgido los IoC (Indicators of Compromise), que permiten perfilar un incidente, crear una línea base para la identificación de diferentes variables asociadas a ese incidente en particular y comparar un dispositivo potencialmente afectado contra dichos parámetros para dar una respuesta rápida y efectiva.

[7] Para el problema de seguridad siempre está latente en los dispositivos móviles, “L*a vulnerabilidad atacaba una debilidad en el código fuente de Android, específicamente en la parte que se encarga de procesar algunos contenidos multimedia*”. Fue descubierta en agosto de 2015 por Zimperium, una empresa de seguridad, y luego fue confirmada por Google. El arreglo ya está en el código de Marshmallow, la versión más reciente de Android, pero eso no garantiza nada por la lentitud con la que suelen llegar los sistemas operativos móviles o los parches para dichas vulnerabilidades. En ese mismo sentido, [7] “Al menos esta vez la vulnerabilidad se conoce incluso una segunda versión y, hasta donde se sabe, no ha sido explotada. Al menos, Google implementó un programa de actualizaciones mensuales para poder reaccionar mejor ante semejantes amenazas. Algo es algo, pero mientras los fabricantes y operadores sigan siendo el cuello de botella que son, el problema seguirá ahí.”.

Otra buena noticia del segundo trimestre de 2020 es una disminución en la cantidad de dispositivos que contenían stalkerware (figura 2) existen varias explicaciones posibles en cuanto a la causa de la disminución significativa que hemos visto desde el cuarto trimestre de 2019.

Figura 2. Afectación de malware en dispositivos. Como se observa en la figura, el Q2 hace parte del cuartil 1 del año 2020 Fuente: Imagen Tomada del Boletín de Karsperky IT threat evolution Q2 2020. Mobile statistics



El adware encabezó la lista con un 48%, una disminución de un punto porcentual con respecto al trimestre anterior. La familia de programas publicitarios Ewind (60,53% de todos los programas publicitarios detectados) fue la más común en el segundo trimestre, seguida de la familia FakeAdBlocker con un 13,14% e Inoco con un 10,17% [16].

[16] El software potencialmente no deseado de tipo RiskTool ocupó el segundo lugar entre todas las clases de amenazas detectadas. Su participación fue del 20%, que es ocho puntos porcentuales menor que en el primer trimestre de 2020 y 21 p.p. menor que en el segundo trimestre de 2019. La mayoría de las variantes de RiskTool detectadas fueron familias SMSreg (44,6% de todo el software potencialmente no deseado detectado), Resharer (12,63%) y Dnotua (11,94%).

Sin embargo, las soluciones para detectar, alertar y generar recomendaciones siguen un poco retrasadas dada la forma de funcionamiento (firmas), lo que genera una oportunidad para establecer otro mecanismo que apoye la reducción de los riesgos.

[17] Los troyanos SMS ocupan el tercer lugar entre todas las amenazas detectadas con un 7,59%. Se cree que esta clase de amenaza está desapareciendo, ya que una cuenta de operador de telefonía móvil es un objetivo mucho menos tentador para los delincuentes que una cuenta bancaria, y ambas pueden controlarse desde un dispositivo móvil. Agent (33,74%), Fakeinst (26,80%) y Opfake (26,33%) fueron las familias más grandes de troyanos SMS detectados. Las tres familias eran más comunes entre los usuarios rusos, lo que es típico de toda la clase de amenazas de troyanos SMS. Los usuarios de Irán lo siguieron, muy por detrás de los rusos. Las familias Opfake y Fakeinst también son líderes en el número de detecciones en dispositivos de usuario final, cada una de las cuales representa el 23% del número total de usuarios únicos atacados por troyanos SMS. La familia Prizmes (21%) y la familia Agent (16%) le siguieron en tercer y cuarto lugar, respectivamente.

[17] Las familias Opfake y Fakeinst se encuentran entre las amenazas móviles más antiguas conocidas por Kaspersky. Es seguro decir que su descubrimiento en la naturaleza es más un eco de campañas de distribución a gran escala pasadas. Esto está respaldado por el hecho de que la mayor parte del malware detectado ya no tenía centros de control en funcionamiento. Dado que el principal medio de distribución de estos troyanos son los sitios web de aplicaciones falsas, se puede suponer que durante el bloqueo es más probable que los usuarios recurran a dichos recursos en busca de contenido gratuito y, por lo tanto, proporcionen a las familias de malware un impulso estadístico.

[8] Otras de las amenazas bien conocidas son el robo de criptomonedas que afecta a Android directamente y el cual se ha reducido, además de la caída del precio de bitcoin y otras criptomonedas, la caída de la criptominería actividades observadas en el cuarto trimestre de 2019 y el primer trimestre de 2020 pueden atribuirse, en gran medida, a la Operación Goldfish Alpha. Esta operación, coordinada por INTERPOL, identifico 20.000 enrutadores pirateados en la región, que supuestamente representaron el 18% de las infecciones de malware cryptomining. A finales de noviembre de 2019, la cantidad de dispositivos infectados se había reducido en un 78%, según INTERPOL.
Así mismo, existe el JavaScript malicioso el cual es utilizado para la minería en el navegador, detectado como JS / CoinMiner, no se recuperó tras la desaparición del infame servicio de minería Coinhive en marzo de 2019. Si bien en el primer trimestre de 2019 cubrieron alrededor del 30% de todas las detecciones de criptomineros, en el primer trimestre de 2020 su la participación se mantuvo justo por encima del 10%, prácticamente sin cambios en comparación con el cuarto trimestre de 2019.

Se vienen presentando diferentes eventos de seguridad sobre los dispositivos Android, sin embargo, las soluciones no son claras y tienden a estar desarticuladas cuando un evento ocurre o se quiere detectar y entregar más opciones a los usuarios finales.

En consideración de la problemática de seguridad en los dispositivos móviles, este trabajo se enmarcó en el siguiente **Objetivo General**

Identificar las amenazas informáticas de tipo Malware bancario o Ransomware Móvil hacia dispositivos Android, con el uso los IOC a través de una herramienta semiautomatizada con el fin de detectar, clasificar y sugerir una propuesta de controles.

Apoyado para el desarrollo total de la tesis de grado en los siguientes **objetivos específicos**:

- Caracterizar los diferentes Indicadores de Compromiso que puedan ser usados o desarrollados en Android en sus últimas 2 versiones más usadas, con el fin de detectar posibles ataques informáticos tipo Malware.
- Proponer un mecanismo de clasificación de acuerdo al nivel de impacto de las amenazas informáticas.
- Diseñar una aplicación que permita la incorporación de Indicadores de Compromisos para la detección de manera semiautomática los diferentes ataques, generando posibles controles.
- Verificar la pertinencia en el proceso de detección, clasificación, y contención rápida a través de la ejecución de la aplicación en Android.

1. Marco Teórico y Estado del Arte

A continuación, presento el Estado del Arte y Marco Teórico el cual dará mayor profundidad a los autores con los cuales logre apalancar mi investigación.

1.1 Estado del Arte

Para el desarrollo de este trabajo de grado se buscaron todos los temas relacionados con los indicadores de Compromiso, basados en Android, e incluyeran técnicas automatizadas basadas en reglas YARA entre otras, en las bases de datos científicas bibliográficas como lo son la IEEE, Science Direct, bibliotecas Unal, Dialnet entre otras; utilizando las palabras en inglés y español, dentro de los buscadores como: YARA, Automatización, Android, Malware, IOC, para lo cual se encontraron más de 25 artículos relacionados con el tema, que guardan relación directa con los IoC, o técnicas de automatización YARA, aplicado en el análisis forense en la afectación de un sistema de información o dispositivo. A continuación, se explica cada uno de ellos ordenado por relevancia del más importante al menos relevante.

Para la realización de este proyecto de grado se han analizado los estudios y proyectos que previamente han tratado de dar solución al problema del malware en dispositivos móviles. De esta manera se puede dar una visión general de las utilidades necesarias para llevar a cabo esta labor y conocer de forma concisa cómo se puede implementar el proceso automatizado de detección de malware para dispositivos móviles, y disminuir los ataques y bloquear comportamientos indeseables de aplicaciones relacionados a los permisos que se le otorgan.

[16] En el Simposio internacional sobre tecnologías para la seguridad nacional, 2018, se ha indicado de muchas de las técnicas encontradas usan diversas metodologías como la teoría de grafos, expuesto en 2018 en la conferencia llevada a cabo en Woburn, MA, USA, Simposio internacional sobre tecnologías para la seguridad nacional (HST). Esta teoría habla que la medición y el registro de IoC de forma aislada no proporcionan una visión precisa del incidente real y, por lo tanto, no facilitan la atribución del ciberataque, La teoría de grafos se ha utilizado para modelar sistemas complejos de diversos tipos y esto

proporciona una herramienta matemática para modelar indicadores de compromiso de sistemas ya que describiría mediante gráficos de manera más precisa el incidente.
Por otro lado, [16] en la búsqueda se encontró una herramienta que utiliza la minería de IOC o MinerIOC, como el usado en la extracción automática de indicadores de compromiso en Twitter. Que es un marco escalable de IoCMiner, para extraer automáticamente la información compartida, en Indicadores de Compromiso especialmente de Twitter y este Utiliza una combinación de teoría de grafos, aprendizaje automático y técnica de minería de texto para lograr su objetivo.

Así mismo, en la década de los 80 cuando nace la informática forense, se desarrollan diversas técnicas que ayudarían en la investigación y esclarecimiento con evidencias de la ocurrencia anómala de ataques en un sistema informático, ya que aún no se conocía la palabra ciberataque. En 1984, fue creado un programa del FBI Conocido como el Programa de Medios Magnéticos, este ahora se llama CART (del inglés computer analysis and response team), o análisis de informática y equipo de respuesta. En 1993 se realiza la primera conferencia anual sobre evidencias de computadoras, y en el 95 se formó la organización de evidencia digital (IOCE).

Por esto, en el avance de sistemas detección [17] desarrollaron a la medida, se creó un sistema para la detección de código malicioso de manera dinámica y estática, lo que hace este modelo es utilizar gran cantidad de datos, para obtener mayor información de los daños y cambios realizados por el código malicioso, el gran problema que surgió según sus autores es que Android no entrega mucha información de sus procesos internos en cuanto a la sesión de permisos a aplicaciones cuando modifican archivos.

Otro problema encontrado en este modelo es que las aplicaciones maliciosas tienden a desconectar el intercambio de datos durante su instalación, que a su vez presentan una mayor complejidad en la solicitud de permisos para poder proveer de más funcionalidades a la aplicación en proceso de instalación a diferencia de las malignas que se enfocan en la forma de realizar daño y presentan exageración en sus solicitudes de permisos.
Como los anteriores, estos autores [18] consideraron el desarrollo de un sistema que permita la caracterización de código malicioso utilizando como factor diferenciador el

aprendizaje de máquina y análisis estático, utilizando las características de los componentes del hardware y de las aplicaciones, usando más de 3000 mil muestras de código malicioso, que fueron recolectadas por la Play Store de google, lo que permite este sistema es detectar, clasificar y ayudar en la detección del elemento malicioso, pero no se evidencia el uso de IoC para ello.

Por otro lado, basados en este estudio [19], se examinaron varias características de Android las cuales fueron solicitudes de permisos y llamados al sistema, todo basado en aprendizaje de máquina, para la detección de código malicioso en los smartphones con Android. Demostraron que controlando las solicitudes de permisos en el dispositivo la tasa de detección en Android es mucho más altos con esta técnica, la precisión fue de más del 80%, esto da una forma confiable para detectar un programa maligno.

Por estas razones anteriores, estos autores [20] buscaron obtener el comportamiento del sistema de más de 216 aplicaciones maliciosas, para así construir un vector de características y así entrenar un clasificador de lenguaje de máquina para realizar la detección de software malicioso, Incluyen entre otras técnicas de clasificación y modelos de predicción las siguientes: árbol de decisión, bosques aleatorios, potenciación de gradiente, algoritmo k-NN, redes artificiales neuronales, máquina de vectores de soporte y aprendizaje profundo. Por medio de técnicas de clasificación de características se seleccionaron las más apropiadas entre un grupo de 337 atributos (llamadas de sistema) y se determinó el peso de estas, descartando las de menor rango para medir el desempeño de los clasificadores, con eficacia y experiencia. El experimento muestra que las máquinas de vectores de soporte, después de seleccionar las características a través del análisis de correlación, superaron a otras técnicas en las que se logró una precisión del 97.16% con recuperación del 99.54% para aplicaciones maliciosas. El estudio también contribuye al identificar el conjunto de llamadas a los sistemas que son cruciales para identificar la intención maliciosa de las aplicaciones de Android.

Al Igual que los autores anteriores, [21] este realizó un estudio comparativo basado en el comportamiento de un programa maligno y las aplicaciones benignas usando sus características estáticas y dinámicas, en el análisis estático, se consideran los permisos necesarios para una aplicación. Usaron las herramientas de almacenamiento en nube la cual es una Sandbox que se usa con el fin de monitorear algunas acciones de la aplicación,

como actividades de red, actividades del sistema de archivos, actividades criptográficas, fuga de información, entre otras, dichas acciones fueron realizadas a través de las llamadas de API dinámicas de las aplicaciones. En ese trabajo se propone implementar una herramienta antimalware para Android que pueda detectar si una aplicación es un dañina o no, antes de la instalación.

[22] para una definición más estándar y que las empresas antivirus y equipos de respuesta a incidentes puedan analizar mejor la información, empresas y aplicaciones como Mandiant, cuyos indicadores de compromiso y Software son abiertos, y cuyos estudios demuestran el crecimiento exponencial de las amenazas el cual se puede obtener en Mandiant Security Effectiveness Report se han dado a la tarea de recopilar dichos incidentes y mejorar los (IODEF) Incidnet Object Descripción Exchange Format, los cuales se encargan de documentar de una manera estándar los IoC. Para lo cual han creado un editor de los IoC y otro para la búsqueda de indicadores de compromiso en el sistema, que se faciliten en una lista ya creada.

Desde la perspectiva de la industria han surgido diferentes modelos de implementación del concepto de IoC. A pesar de que no existe un estándar definido, y no hay ninguno que se aplique en móviles a continuación se puede ver algunos de los modelos más importantes que pueden ser empleados dependiendo de las necesidades que se tengan como se quiera aplicar los indicadores más eficientes para cada caso:

[23] Esta es otra iniciativa que está respaldada por algunos de los principales fabricantes de soluciones de seguridad y está orientada hacia la definición y estandarización de un conjunto de representaciones de información y protocolos para gestionar la necesidad de analizar, modelar y compartir datos de inteligencia contra amenazas informáticas. Está compuesto por tres subcomités: STIX (Structured Threat Information Expression, TAXII (Trusted Automated Exchange of Indicator Information) y CybOX (Cyber Observable Expression.

Finalmente se crea un estándar con el cual todos pudieran usar la información, en diciembre de 2007 se publicó la RFC 5070, que contiene la descripción básica del esquema XML para el registro de variables técnicas relacionadas con incidentes conocidos para ser

empleados principalmente por centros de respuesta a incidentes (CSIRT), orientado hacia la automatización en el procesamiento de datos de incidentes y la gestión de un formato común para construir herramientas interoperables para la gestión de incidentes [24].

Después de ahondar en los diversos artículos y modelos propuestos de la literatura descrita en la bibliografía, se puede ver claramente que no existen la aplicación o uso eficiente de los indicadores de compromiso enfocados en dispositivos móviles Android o que estos no están automatizados mediante una herramienta o aplicación que se ejecute automáticamente en ellos.

1.2 Marco Teórico

Cuando hablamos de un indicador de compromiso o IoC (del inglés Indicator of Compromisees) es una porción de software que permite la identificación de algún patrón que indica que el sistema posiblemente este comprometido, lo que genera la descripción de un posible incidente de Ciberseguridad, puede ser un código malicioso, que ha afectado un dispositivo, equipo de cómputo, equipo móvil celular, tableta o cualquiera que este expuesto a Internet; se está en constante Riesgo, por amenazas cibernéticas, que encuentran vulnerabilidades, en los dispositivos y los controles, no son suficientes para la protección del smartphone, siendo presa fácil de ciberataques, en nuestros dispositivos Android por lo anterior los indicadores de compromiso usan patrones de comportamientos del código malicioso, estos patrones se clasifican y se describen muy bien y en orden, aclarando su afectación en cada uno delos archivos del sistema y se convierten en indicadores de compromiso y se esquematiza durante el análisis de un incidente de seguridad, de manera que dicho análisis se pueda volver a utilizar para identificar cuando se produzca de nuevo, esto sirve para poder realizar un análisis forense y determinar si el comportamiento es similar a un ataque ya presentado anteriormente, los indicadores de compromiso se desarrollan después de afectado por el ciberataque en el dispositivo, siendo la aplicación de estos IoC pasivos, mas no aplicado antes o durante la afectación [9].

Por lo anterior, para comprender un poco más los componentes de este esta investigación de grado a continuación se detalla algunos de los términos utilizados en esta investigación.

1.2.1 Términos usados en los indicadores de Compromiso

[10] cuando se presenta un Incidente de Seguridad es necesario actuar rápidamente, para ello, se entiende como un evento que podría generar daños en un sistema de información o un dispositivo como teléfono celular, equipo de cómputo, servidor, dispositivo de red, en este caso compromete un sistema informático a tal punto que se hace necesario tomar medidas, de contención, para evitar perdida, robo o sustracción de información relevante para un organización o persona.

[14] De ahí que los estándares son de gran relevancia para la identificación de cada uno de los patrones de un incidente de seguridad y así poder aplicar de manera correcta las contenciones o lograr identificar correctamente el atacante, por esta razón la importancia de la IETF que es Grupo que se encarga de crear los estándares abiertos, tanto para la internet como para dispositivos de red, y uno de sus estándares plasmados en la guía de referencia RFC5070, que habla precisamente de los estándares IoC como estándar en la clasificación y descripción de estos, Así como existe el Openioc, que es un estándar abierto para la creación de indicadores de compromiso basado en el formato expedido por le IEFT, el cual es ampliamente usado y que para esta tesis será relevante.

[25] para este estandar OpenIOC que es un marco abierto, diseñado para compartir información de inteligencia de amenazas en un formato legible por máquina. Fue desarrollado por la firma estadounidense de ciberseguridad MANDIANT en noviembre de 2011. Está escrito en extensible Markup Language (XML) y se puede personalizar fácilmente para obtener inteligencia adicional para que los respondedores de incidentes puedan traducir sus conocimientos a un formato estándar. Las organizaciones pueden aprovechar este formato para compartir los indicadores de compromiso (IoC) más recientes relacionados con las amenazas con otras organizaciones, lo que permite la protección en tiempo real contra las amenazas más recientes.

[15] Para esto los indicadores de compromiso son construidos mediante técnicas abiertas en editores hechos para tal fin, bajo los estándares de la IETF (Internet Engineering Task Force), el cual se encuentra en la guía de referencia rfc5070, la cual es un standard que, apoyado por una comunidad abierta, coopera para que todos los fabricantes, investigadores, desarrolladores, inventores trabajen bajo unos marcos de referencia donde puedan interactuar los diferentes dispositivos.

Aunque tener un IoC es relevante y ayuda en la clasificación rápida de un ciberataque, este por sí solo no impacta, protege ni reacciona durante el incidente, por lo que es importante la aplicación de una técnica automatizada, como anteriormente se describió, basado en Reglas YARA, que lo que hace es: previa carga de un fichero XML, con los IoC, identificar el comportamiento de los distintos sistemas, tareas, procesos en el dispositivo y ejecutar una secuencia para impedir que el ataque se efectué, en tiempo real, no después de sucedido el incidente, logrando una detección, clasificación y contención rápida con base en comportamientos analizados de incidentes.

1.2.2 Indicadores de Compromiso para Android

[25] las empresas de seguridad informática (como IBM) han utilizado el IOC para referirse a los ciberataques a la evidencia digital forense. Este tipo de evidencia digital forense puede reportar anomalías, como direcciones IP, dominios, archivos y pistas digitales. Estas anomalías parecen ser capaces de detectar la conexión entre una red de ciberataques y un ciberatacante sospechoso a través de herramientas de gestión de endpoints. Las herramientas de gestión de terminales pueden detectar incidentes de seguridad y reparar el daño causado. Los IOC pueden capturar detalles inesperados de acceso a la red basados en direcciones IP asociadas con ciertas ubicaciones geográficas. Las empresas de ciberseguridad como Kaspersky Lab pueden divulgar IOC para que las organizaciones puedan identificar los rastros de grupos financieros en sus ciberataques, como Metel, GCMAN y Kabanak 2.0.41.

En los últimos años, empresas de seguridad de la información como IBM, Intel y CrowdStrike han utilizado el término "indicador de ataque (IoA)" para referirse a la evidencia digital forense de ciberataques en curso o posibles ataques de código malicioso. En el futuro, habrá herramientas de protección de objetivo final que puedan detectar incidentes de seguridad y reparar el daño causado. Para CrowdStrike, IOC se refiere al malware de IoA, firmas, exploits, vulnerabilidades y direcciones IP, ejecución de código de referencia, persistencia, sigilo, control de comandos y movimiento de procesos afectados.

1.2.3 Indicadores de Compromiso Más Frecuentes

[26] En la búsqueda por detectar violaciones de datos con mayor rapidez, los indicadores de compromiso pueden actuar como importantes alarmas para identificar la evolución de un ataque, e intentar mitigarlo en sus primeras etapas. Algunos de los IoC más empleados son:

Tráfico Inusual de la Red: es considerado uno de los mayores signos reveladores de que algo anda mal. Cualquier movimiento extraño que se detecte en el tráfico debe ser un signo de alarma para los administradores. Si bien es posible que no sea un ataque, hay que verificar que no haya un punto vulnerable que pueda ser un lugar de acceso para ello.

Anomalías en Cuenta de Usuario: los cambios en el comportamiento de los usuarios pueden indicar que la cuenta de usuario en cuestión está siendo utilizada por otra persona. La observación de cambios, como el tiempo de actividad, los sistemas a los que se accede, el tipo o el volumen de información que se maneja, proporcionará una indicación temprana de una violación.

Irregularidades Geográficas: si se detectan conexiones de usuarios en diferentes ubicaciones geográficas que no tienen relación con la entidad o bien que un mismo usuario se conecta desde diferentes direcciones IP, constituye una alerta indicativa de que pueden existir problemas. La mayoría de las veces, este es un síntoma de un ataque que utiliza un conjunto de credenciales comprometidas para iniciar sesión en sistemas confidenciales.

Banderas Rojas: el inicio fallido de sesión utilizando cuentas de usuario que no existen, a menudo indica que alguien está tratando de adivinar las credenciales y obtener autorización; de igual modo, el éxito de inicio de sesión después de buen tiempo de intentos fallidos, puede proporcionar indicios de que en realidad no es el propietario de la cuenta el que está accediendo a los datos.

Incremento Extraordinario de Consultas a Base de Datos: cuando un atacante intenta extraer información valiosa de una base de datos, generará una enorme cantidad de volumen de lectura, que será mucho más alto de lo que normalmente ocurre en transacciones ordinarias, lo que constituye un indicador de alerta de que se está extrayendo información valiosa.

Tráfico por Puertos Inusuales: los atacantes a menudo se aprovechan de puertos inusuales para comprometer dispositivos y redes. El empleo por una aplicación de un puerto poco frecuente podría constituir una señal de alarma.

Cambios Sospechosos del Sistema de Archivos: cuando un dispositivo es comprometido, suele instalarse alguna herramienta de rastreo de paquetes para recolectar datos en la red; si bien las posibilidades de detectarla son menores, existe una buena posibilidad de alertar los cambios en el sistema que la contiene (que la alberga), pues para lograr su permanencia, el atacante debe realizar cambios en el registro de archivos. Definir qué se supone debe contener un registro de archivos limpio, y alertar sobre cambios, puede aumentar drásticamente el tiempo de respuesta del equipo de seguridad.

Anomalías en DNS: detectar un gran aumento en las solicitudes DNS de un host específico a servidores externos puede servir como un buen indicador de una actividad potencialmente sospechosa. Los patrones únicos de este tráfico pueden ser reconocidos y es un enfoque estándar para la identificación de un IoC.

De forma general, aprender a gestionar los IoC aportará conocimiento de para proteger la información que soporta una infraestructura de comunicaciones. El uso de estos indicadores permitirá disponer y mejorar una serie de herramientas, que pueden ser claves en la resolución y prevención de incidentes de seguridad informática.

La potencia de los indicadores de compromiso se encuentra en la compartición de información relevante de un incidente, dando libertad a los encargados de gestionarlo para aplicar esta información en sus sistemas. El tiempo que no se emplee en repetir el trabajo que otros ya han realizado, probado y compartido en un IoC de confianza, es el tiempo de ventaja para minimizar los riesgos de incidentes.

Los IoC crean una línea base para la identificación de diferentes variables asociadas a incidentes o ataques de seguridad informática, que permiten comparar un dispositivo potencialmente afectado contra dichos parámetros para dar una respuesta rápida y efectiva.

1.2.4 Características de los Indicadores de compromiso para Android:

[2] Como sugiere su nombre, los Indicadores de Compromiso (IoC) son datos generados como resultado de ciertas actividades en nuestro sistema que pueden proporcionarnos información sobre el comportamiento, las características o la descripción de las amenazas. En este sentido, IoC puede usarse como evidencia, lo que nos permite confirmar que nuestro equipo ha sido comprometido por malware, pero también es información que puede usarse para prevenir futuros ataques. En otras palabras, puede dar indicaciones dañinas en forma de nombres de archivos, nombres de procesos en el administrador de tareas, direcciones URL o IP, comportamientos anormales en las comunicaciones web e intentos fallidos de inicio de sesión.

Para comprender cómo funciona el malware y cuál es su objetivo final, una de las tareas que realizan los investigadores de seguridad es analizar y monitorear las diferentes amenazas que forman parte de las actividades que realizan los actores maliciosos. Estas amenazas pueden ser nuevas o conocidas. Si son nuevos, el objetivo será comprender cómo funcionan, y si se han informado anteriormente, el objetivo es monitorear su evolución y posibles cambios. Los indicadores de compromiso se utilizan generalmente para realizar esta tarea.

Las características principales de un indicador de compromiso son:

- Qué recursos del sistema utiliza
- Cómo manipula y qué cambia del sistema para poder llevar a cabo sus acciones
- Cuál es la finalidad del malware y sus componentes si los hay

Dado que el malware necesita realizar varias tareas en el sistema para lograr sus objetivos, esto rara vez sucede sin dejar evidencia de su existencia o pistas que nos ayuden a detectar actividad sospechosa en el sistema. Demuestre que hemos sido víctimas de una infección. La evidencia que dejan estos rastros o amenazas en el sistema es un indicador de daño. Las empresas de seguridad utilizan estos IoC para desarrollar archivos de configuración de modo que las soluciones automatizadas (como los productos anti-malware) puedan detectar infecciones en la etapa más temprana.

1.2.5 Como se crea un indicador de Compromiso para Android:

Esto se hace analizando cuidadosamente la función y el comportamiento de la muestra de malware. La muestra en sí es una IOC: la práctica estándar de la industria es utilizar un algoritmo hash para generar un identificador único de cada muestra. El identificador (hash) es único y no hay dos muestras de malware con datos diferentes y el mismo identificador.

Figura 3 Tomada de ESET ejemplo de un Hash, de un archivo con Malware.

Hashes

Campaña "MSI overload"

SHA-1	Description	ESET detection name
D8C6DDACC42645DF0F760489C5A4C3AA686998A1	MSI installer	JS/TrojanDownloader.Banload.ABD
01ECACF490F303891118893242F5600EF9154184	MSI loader	Win32/Spy.Vadokrist.T
F81A58C11AF26BDAFAC1EB2DD1D468C5A80F8F28	Vadokrist banking trojan	Win32/Spy.Vadokrist.T

Otro

SHA-1	Description	ESET detection name
8D7E133530E4CCECE9CD4FD8C544E0913D26FE4B	Vadokrist banking trojan	Win32/Spy.Vadokrist.AF
AD4289E61642A4A724C9F44356540DF76A35B741	Vadokrist banking trojan	Win32/Spy.Vadokrist.T
BD71A9D09F7E445BE5ACDF412657C8CFCE0F717D	Vadokrist banking trojan	Win32/Spy.Vadokrist.AD
06C0A039DEDBEF4B9013F8A35AACD7F33CD47524	Downloader (MSI/JS)	JS/TrojanDownloader.Banload.AAO

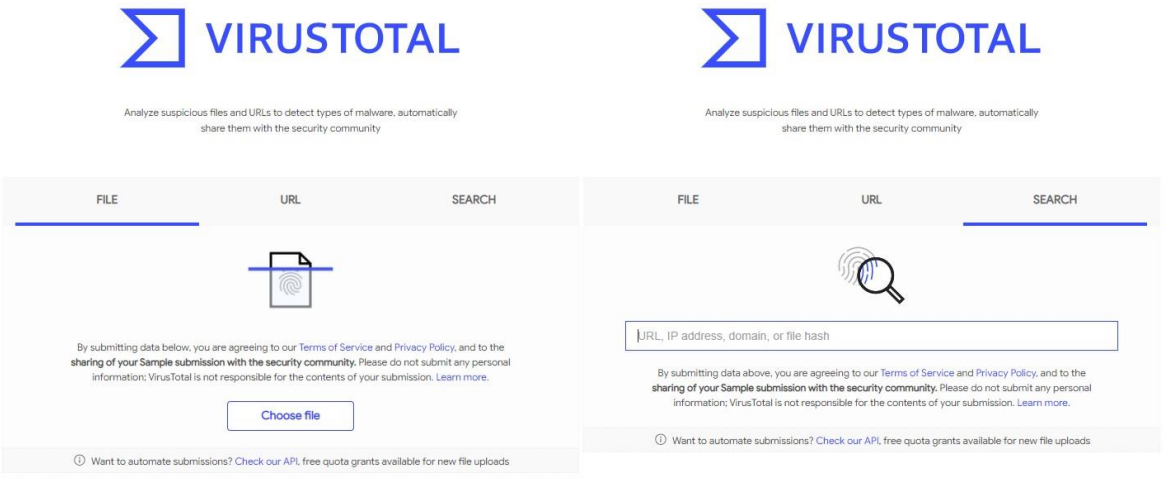


Figura 4. El algoritmo hash no es el secreto de propiedad de la empresa de seguridad. Cualquier investigador o usuario con un cierto nivel de conocimiento puede usar una herramienta para generar un valor hash a partir de una muestra y usar el valor hash para

buscar información sobre Kazajstán en bases de datos públicas o plataformas de análisis de amenazas en línea (como VirusTotal o herramientas similaresTomado de Virus Total.

En cada análisis publicado, el valor hash de la muestra analizada generalmente se incluye en el informe. De esta forma, otras entidades pueden utilizar estos indicadores de compromiso para incorporarlos al sistema y realizar sus propias investigaciones, que a menudo aportan nuevos datos en la distribución de malware específico.

Es importante mencionar que en una misma actividad de malware se pueden detectar decenas o incluso cientos de variantes de un mismo malware. Por ejemplo, el cambio más común es la adición de una nueva dirección para comunicarse con el servidor C&C, lo que hará que cambie el valor hash de la muestra.

1.2.6 Datos y direcciones IP como complemento de los Indicadores de Compromiso:

[1] No es raro que se detecten actividades maliciosas en cualquier red a través de sistemas de detección de intrusos y monitoreo de tráfico. En algunos casos, cuando una gran cantidad de tráfico de datos en la red fluye hacia servidores externos o servidores pertenecientes a la organización, se activarán las alarmas para estos sistemas. Esto también puede ocurrir entre computadoras conectadas a la red local. Este extraño movimiento de datos y las visitas a páginas web anormales también pueden ser signos de daño.

Cuando analizamos malware, queremos saber la dirección IP del servidor de comando y control (C&C) con el que se está comunicando. Los atacantes utilizan estos servidores para diferentes propósitos. Por ejemplo: enviar comandos a la computadora infectada para controlar de forma remota el malware; recibir informes detallados sobre el sistema infectado; robar información útil (incluidas contraseñas, documentos con información confidencial, etc.) de la computadora o sistema infectado, o incluso descargar otra amenaza al sistema infectado (como suele hacer Emotet Trojan).

1.3 Que es un Malware:

[4] El malware es un tipo de programa malicioso, que puede afectar cualquier tipo de software sin el conocimiento del usuario, mediante acciones que intencionalmente causan daño al sistema informático. El malware es un tipo de código maligno diseñado para robar las credenciales y contraseñas bancarias de los usuarios. Por ejemplo, pueden ser caballos de Troya que existen en computadoras de escritorio o dispositivos móviles. Son un tipo de malware cuya finalidad es robar nuestras cuentas bancarias. La realidad es que muchos usuarios hoy en día usan aplicaciones móviles para acceder a cuentas bancarias, realizar pagos o simplemente verificar el estado de su cuenta. Ahora, los piratas informáticos pueden usar esto para llevar a cabo ataques dirigidos.

1.3.1 Malware Bancario:

Según los informes realizados por las distintas compañías de firmas de Antivirus, los ataques de malware bancario están especialmente dirigidos a usuarios corporativos. Prestan más atención a las empresas y los usuarios en el lugar de trabajo. En concreto, el 35% de todos los ataques de este tipo están dirigidos a usuarios corporativos. Hasta ahora, las cifras de otros años suponían aproximadamente un 24-25% del total, y estamos hablando de un crecimiento importante. La mayoría de las familias de malware del sector bancario y no bancario tratan de explotar la crisis sanitaria mediante actividades fraudulentas, en las que su software malicioso se distribuye como si fueran aplicaciones de rastreo de virus. [5]

1.3.2 Familias de Malware Bancario para Android:

[4] han nacido tres nuevas familias de malware bancario para dispositivos Android, y los malware conocidos como Cerberus y Anubis Bankbot siguen siendo las familias de software más populares y activas.

[4] En 2020, apareció BBTok este es un tipo de malware bancario utilizado en computadoras El malware migró rápidamente a los dispositivos móviles. Además, el ransomware se ha convertido en una moda. Puede cifrar los archivos de la víctima y exigir un rescate. cifra y roba estos archivos para pedirle a la víctima que pague más para evitar que se publique el contenido de los archivos. Esta técnica se llama doxing.

[4] Esta nueva estrategia es particularmente exitosa para las empresas que tratan con datos confidenciales de clientes y no quieren que los datos se publiquen eventualmente en Internet. En resumen, 2020 es el año del malware bancario de Android y del ransomware de escritorio, y esta tendencia continúa en 2021, porque el ransomware es el malware más rentable y uno de los más fáciles de desarrollar.

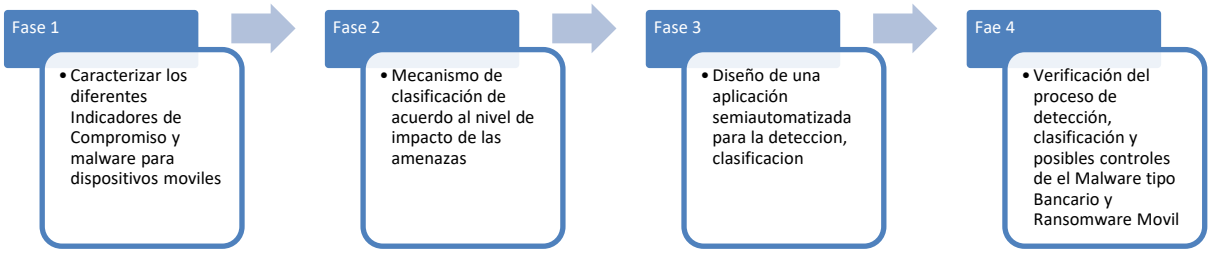
2. Metodología y Resultados

Para este apartado, la metodología y los resultados se presentan en el mismo capítulo, con lo cual, una vez se ha defino el *cómo* se realizó la actividad, se entregan los respectivos resultados y análisis de los mismos.

La metodología utilizada fue el estudio descriptivo donde se referencian las técnicas usadas frecuentemente en el medio y por organizaciones con estándares para las mismas, adicional con metodología de búsqueda, experimentación, desarrollo y documentación.

La metodología se ha dividido por fases, en donde cada fase corresponde a un objetivo específico.

Figura 5. Metodología dividida por fases, en dónde cada fase corresponde a un objetivo específico. Fuente: Construcción propia



2.1 Fase 1: Caracterizar los diferentes Indicadores de Compromiso y malware para dispositivos móviles

Para poder dar cumplimiento a la fase 1 de esta tesis, es necesario dividirlo 5 actividades en las cuales se identificaron y caracterizaron tanto los IOC como el Malware tipo Bancario, que afecta los dispositivos móviles con Android en sus últimas dos versiones más usadas:

- Actividad 1: Selección de las versiones Android con las que se Caracterizaran los diferentes IOC y Malware.
- Actividad 2: Identificación de Malware de tipo bancario
- Actividad 3: Caracterización de Malware Bancario para Android según su afectación y propagación

- Actividad 4: Caracterización de los IOC para dispositivos móviles Android versiones 8 y 9
- Actividad 5: IOC para dispositivos móviles Android Versiones 8 y 9.

2.1.1 Selección de las versiones Android con las que se Caracterizaran los diferentes IOC y Malware

En el mercado existen gran variedad de versiones del sistema operativo Android y esos se actualizan con frecuencia y constantemente, es por esto de la importancia de conocer el porcentaje de uso de cada versión y así obtener las dos últimas con más uso en el mercado, y así trabajar en el desarrollo de este trabajo de grado con las últimas dos versiones. Para la selección de las versiones, se ha construido una tabla referencial (tabla 1) que permite visualizar como se mueve el mercado de las versiones Android:

Nombre de la Versión	**Número de versión**	**Nivel de Uso en el mercado**
Nombre de la Versión o versionamiento numérico	Numero de Versión	% de uso cuantos lo utilizan

Tabla 1. Versiones Android y su uso para dispositivos móviles. Construcción propia

Consecuentemente con lo anterior, para la caracterización de los IOC para la detección de Malware en dispositivos móviles fue necesario identificar y caracterizar el Malware que afecta los dispositivos Android en sus últimas 2 versiones, que, para la ejecución de este proyecto, se tomó como referencia.
[50], en el mundo hay aproximadamente 3000 millones de dispositivos Android, repartido de la siguiente manera (tabla 2) por versión de uso: Tabla 2. en la cual se relacionan la mayor parte de versiones Android y su uso. Fuente [50]

VERSIÓN DE ANDROID	PORCENTAJE
ICE CREAM SANDWICH (4.0)	0,2%
JELLY BEAN (4.1 - 4.3)	1,7%
KITKAT (4.4)	4%
LOLLIPOP (5.0 - 5.1)	9,2%
MARSHMALLOW (6.0)	11,2%
NOUGAT (7.0 - 7.1)	12,9%
OREO (8.0 - 8.1)	21,3%
PIE (9.0)	31,3%
ANDROID 10 (10.0)	8,2%

Tabla 2. versiones de Android por porcentaje de uso a nivel mundial. [50]

Resultado de la actividad 1 de esta fase:

En consecuencia, y como resultado de la caracterización de las versiones Android con mayor distribución y ultimas 2 más usadas en el mercado mundial, a continuación, en la siguiente tabla 3 se puede apreciar la selección de las versiones a trabajar:

Nombre de la Versión	Número de versión	Nivel de Uso en el mercado
OREO	**8.0**	**21,3%**
Pie	**9.0**	**31,3%**

Tabla 3. Últimas dos versiones Android más usadas en el mercado. Fuente [50]

Por lo anterior y para el desarrollo de este trabajo de grado, se tomaron las versiones Android 8 y 9 por ser las versiones más usadas y disponibles al 2020 para ser desarrolladas durante los laboratorios y obtener así los resultados esperados.

2.1.2 Identificación de Malware de tipo bancario para ser usado en la detección y contención en dispositivos móviles Android.

En esta actividad, para la identificación y clasificación de las amenazas más representativas para Android se analizaron los boletines de amenazas de 3 organizaciones reconocidas de firmas antivirus, las cuales entregan un compendio de estas amenazas, en ese sentido se tomaron las siguientes organizaciones de seguridad como referentes:

- McAfee
- ESET
- KARSPERSKY

Se continuo y, se propuso para este trabajo de grado una clasificación de variables de tipo Malware, se clasificaron según su afectación y forma de infección; una vez clasificado se tomaron los 4 Malware con mayor tasa de infección y propagación para realizarle los IoC para dar cumplimiento, esto, con el fin de ser probados en la herramienta semiautomatizada en un laboratorio controlado. En la tabla 4 se puede apreciar los resultados obtenidos, para lo cual, se buscaron los siguientes campos:

- **Nombre de la variable:** nombre del malware que se va a clasificar
- **Descripción:** descripción del malware y su comportamiento y que hace en el sistema infectado
- **Tipo:** tipo de Malware con el cual se identifica si es troyano, bancario gusano etc.
- **Afectación:** afectación que realiza el malware en el dispositivo
- **Forma de infección:** forma por la cual se infecta el dispositivo, por envió de mensaje, por descarga de app

Resultado de la caracterización del Malware Bancario en la siguiente tabla, que contiene Nombre, descripción del malware, tipo, afectación, forma de infección.

A continuación (tabla 4), se presenta parte de la caracterización de las diferentes variables:

NOMBRE DE LA VARIABLE	DESCRIPCION MALWARE	TIPO	AFECTACION	FORMA DE INFECCION
Gravity RAT	software malicioso que permite a sus operadores obtener control remoto del dispositivo infectado. Esto es lo que se conoce como una herramienta de acceso remoto (Remote Access Tool)	Troyano Remote Access Tool	Control Remoto del Dispositivo, permite la ejecución remota de código, explorar el sistema de ficheros de la víctima y acceder a su contenido, registrar las pulsaciones de teclas, tomar capturas de pantalla y grabar audio	Por medio de APP para leer revistas de dibujos animados o Comics
Cerberus	la aplicación maliciosa solicita permisos al usuario lo cual permite recibir eventos generados por la aplicación que se encuentra ejecutándose en primer plano, incluyendo el nombre de paquete de dicha aplicación. Con esta información, el *malware* es capaz de detectar cuando una aplicación es iniciada por parte del usuario, y de esta forma mostrar una ventana falsa solicitando las credenciales de acceso a la entidad bancaria.	Troyano de Acceso Remoto (RAT)	Una vez que el usuario instala la aplicación maliciosa y la inicia por primera vez, ésta solicita al usuario que le de permisos de accesibilidad. Estos permisos permiten al malware recibir eventos generados por otras aplicaciones que se encuentren ejecutando en primer plano. Y así mediante engaño mostrar una ventana falsa puede ser de la aplicación de banco instalada y así roba las credenciales. Robo de patrón de desbloqueo y códigos de Google Authenticator	distribución del APK malicioso

Anubis Bankbot.	Este Malware se descarga en una APP para descargar videos de Google Play una vez se instala y se ejecuta en segundo plano hace un llamado al servidor de comando y control para descargar el resto de la APK así se instala y toma completo control del dispositivo robando usuarios y contraseñas y monitoreando y enviando información de todo lo ejecutado, así como datos del dispositivo.	Troyano	Una vez que se ejecuta en el dispositivo de la víctima se comunica remotamente en segundo plano con su servidor comando y control («Command and Control «, C&C o C2). La aplicación también espera la respuesta del C&C remoto para recibir la orden de obtener el APK final y de esa manera troyanizar el dispositivo completamente.	Como APP en Google Play con el nombre de Bankbot “Downloader for videos”
Eventbot	Malware para robo de credenciales mediante inyección de phishing (sobreescritura). incluye la posibilidad de registrar eventos de accesibilidad ocurridos en el sitio afectado. Adicional también presenta algoritmo de cifrado	Troyano	Las aplicaciones bancarias aprovechan los permisos de accesibilidad y abusan directamente de ellos, por lo que los eventos que ocurren en las aplicaciones bancarias afectadas por malware se registran y envían al servidor de control, especialmente si estos eventos están relacionados con cambios de texto, pues esto es muy probable que el nombre de usuario y campos de	URL para la descarga de contenido. Por medio de cadenas de Whatsapp, correos electrónicos.

			contraseña de un formulario de inicio de sesión legítimo. roba contraseñas, datos privados y hace de keylogger	
BlackRock	robo de credenciales bancarias se lleva a cabo con la estrategia habitual basada en inyecciones web u 'overlays', que son mostradas al usuario inmediatamente después de que esta abra la aplicación de la entidad.	Troyano Bancario	permite a los atacantes recopilar los eventos de accesibilidad que se producen en el dispositivo, especialmente aquellos que se producen en la aplicación de la entidad bancaria de la víctima. De esta forma, este banker puede robar las credenciales a través de técnicas similares al keylogging en sistemas de escritorio.	mensajes enviando un comando al teléfono. Por medio SMS, listas de contactos del teléfono.
teatv.apk	El malware instala un servicio de accesibilidad en el teléfono para controlar toda la actividad del mismo, con el fin de detectar la apertura de aplicaciones bancarias	Troyano Bancario	Detecta apertura de aplicaciones bancarias y roba credenciales enviándolas a un servidor de comando y control.	Por medio de una APK que se descarga y ofrece peliculas gratis.
Alien	suplantar una entidad bancaria y robar las credenciales de acceso, esta nueva "evolución" ha ampliado su «target» a un total de más de 200 aplicaciones para el sistema Android. Como pueden ser	Troyano Bancario	Registro de teclas pulsadas (keylogger). Instalación de otras aplicaciones. Desvío de llamada. Acceso a los datos de localización.	Descarga de aplicaciones de terceros sin firma; correo electrónico hasta por SMS. Muchas muestras de la aplicación han sido distribuidas

	aplicaciones de tal importancia hoy en día como Facebook, WhatsApp, Twitter o Instagram. En el informe de análisis que ha publicado Threat Fabric puede ser consultado el listado de todas las aplicaciones vulnerables al malware.		Robo de agenda de contactos.	utilizando el nombre de “Coronavirus”
Anubis	Esta familia de malware ha estado realizando conocidos ataques de superposición mediante la combinación de funciones avanzadas como la capacidad de transmitir pantallas, grabar sonidos, buscar archivos de forma remota, capacidades de registro de teclas y la capacidad de funcionar como un proxy de red. Estas características lo convierten en un malware bancario efectivo y una herramienta potencial para espiar.	Troyano Bancario	Superposición: estática (codificada en bot) Superposición: dinámica (basada en C2) Registro de teclas Colección de lista de contactos Transmisión de pantalla Grabación de sonido Recolección de SMS: reenvío de SMS Bloqueo de SMS Envío de SMS Colección de archivos / imágenes Llamadas: solicitud de USSD	Campañas de Google Play: Esto incluye Evitar los mecanismos de seguridad de Google Play y propagar el troyano utilizando la tienda oficial de aplicaciones. Campañas de spam: Esto utiliza SMS o correos electrónicos con una solicitud para instalar o actualizar alguna aplicación

			Ransomware: Cryptolocker Acciones remotas: borrado de datos Acciones remotas: Proxy de back-connect Notificaciones: notificaciones push Resiliencia C2: canales de actualización de Twitter / Telegram C2	legítima que se vincula al malware. Redirección web: El uso de publicidad en sitios web, sitios pirateados, intercambios de tráfico atrae a la víctima a una página de destino falsa que contiene una aplicación de malware.
Hydra	malware que realiza ataques de superposición de pantallas mediante la combinación de funciones avanzadas con la capacidad de transmitir pantallas	Troyano Bancario	Visualización de la pantalla del teléfono en tiempo real. Instalación remota de aplicaciones. Funcionalidades de RAT (Troyano de acceso remoto). Superposición de pantallas bancarias falsas. Interceptación y robo de mensajes SMS. Funcionalidad de Back-connect proxy.	Activación y descarga de complementos de flash player, aplicaciones de terceros sin firmas y verificación. Apk Commerzbank Security

			Imposibilidad de desinstalar la aplicación desde el apartado de aplicaciones.	
Ginp	este malware Ginp se Instala en el móvil, sobrepondrá una pantalla calcada a la del banco por encima de la app legítima, pero con una finalidad distinta que es el robo de las credenciales del usuario. Primero pedirá las credenciales para acceder y después la tarjeta, con su fecha de caducidad y el número CVV. El usuario creerá que está usando la app del banco, pero estará dando sus datos a los ladrones.	Troyano Bancario	secuestra la lista de contactos y reenvía el enlace a otros usuarios. Superposición: dinámica (superposiciones locales obtenidas del C2) Recolección de SMS: listado de SMS Recolección de SMS: reenvío de SMS Colección de lista de contactos Listado de aplicaciones Superposición: actualización de la lista de objetivos SMS: Enviando Llamadas: desvío de llamadas Resiliencia C2: Lista auxiliar C2 Autoprotección: ocultar el icono de la aplicación	Se distribuye por medio de mensajes SMS, se camufla como una actualización de Android a la versión 10.

			Autoprotección: evitar la eliminación Autoprotección: detección de emulación	
Gustuff	Gustuff infecta los smartphones Android a través de mensajes SMS que contienen enlaces a archivos de Paquete Android (APK) maliciosos. Una vez que se completa la infección, el malware abusa del Servicio de Accesibilidad para aprovechar su función de Sistemas de Transferencia Automática en un dispositivo infectado. Esta capacidad le permite al troyano eludir los mecanismos de seguridad cuando una víctima interactúa con aplicaciones bancarias, así como con tiendas online, sistemas de pago y servicios de criptomonedas.	Troyano Bancario	Gustuff usa notificaciones falsas para robar las credenciales de pago de los usuarios o sus datos personales. El troyano puede usar el Servicio de Accesibilidad para completar automáticamente los campos de pago para realizar transacciones ilícitas, y enviar información confidencial sobre el dispositivo infectado a su servidor de comando y control (C&C), leer y enviar mensajes SMS y restablecer la configuración de fábrica del dispositivo.	infecta los teléfonos a través de SMS que contienen enlaces a archivos maliciosos.
BlackRock	BlackRock, que se encarga de extraer contraseñas y datos de tarjetas bancarias.	Troyano Bancario	detectar cuándo un usuario intenta interactuar con una aplicación legítima y mostrar una ventana falsa en la parte superior que recopila los datos	Mensajes de Texto, Cadenas de Whatsapp.

			de inicio de sesión y los datos de la tarjeta de la víctima antes de permitirle al usuario para ingresar a la aplicación legítima prevista. Interceptar mensajes SMS. Contactos de spam con SMS predefinidos. Iniciar aplicaciones específicas. Mostrar notificaciones push personalizadas Sabotear aplicaciones antivirus móviles y más.	
Mispadu	Mispadu es una familia de malware que apunta principalmente a Brasil y México Está escrito en Delphi y ataca a sus víctimas utilizando el mismo método que describimos en las otras familias de esta serie, es decir: desplegando falsas ventanas emergentes y tratando de persuadir a las	Troyano bancario	Por su funcionalidad de backdoor, Mispadu puede realizar capturas de pantalla, simular acciones de mouse y teclado, además de registrar las pulsaciones de teclado. Puede actualizarse a través de un archivo de Visual Basic Script (VBS) que se descarga y ejecuta de manera automática.	spam y publicidad maliciosa.

	posibles víctimas para que divulguen información confidencial.			

Tabla 4. Resultado de la caracterización del Malware Tipo Bancario que afecta dispositivos Android en sus dos últimas versiones más usadas para el 2020 (8 y 9). Construcción propia.

Resultado actividad 2 fase 1:

El resultado de la anterior tabla 4 referimos el Modus Operandi del Malware Bancario para alcanzar sus objetivos maliciosos, los troyanos bancarios Android sofisticados suelen seguir todos o la mayoría los siguientes pasos:

1. Engañar a la víctima para que instale malware sin saberlo usando varias técnicas como envió de mensajes de texto, cadenas de WhatsApp entre otros.
2. Obtener los permisos necesarios para poder (leer más en Funcionalidad y permisos y técnicas de sigilo y evasión de detección).
3. Opcional: Asegura la persistencia en el dispositivo tratando de evadir solicitando permisos especiales para escribirse en memoria o en los archivos del sistema.
4. se ejecutan en segundo plano hasta que se inicie la aplicación legítima u objetivo o engañe la víctima para que lance esa aplicación para poderla afectar y robar la información.
5. Se superpone a la aplicación legítima con una pantalla de phishing solicitando credenciales de inicio de sesión o detalles de tarjetas de crédito / débito. Para que el usuario victima las ingrese y robarlas.
6. Recolecta las credenciales ingresadas o los detalles de la tarjeta de crédito / débito y los envía al servidor C&C.
7. Utilizan permisos de SMS para interceptar la contraseña de un solo uso (OTP)
8. Lleva a cabo transacciones fraudulentas utilizando la cuenta bancaria de la víctima y / o vender credenciales robadas en el mercado negro.

2.1.3 Caracterización de Malware Bancario para Android según su afectación y propagación según el número de dispositivos afectados por cada variante, al dispositivo móvil Android en sus dos versiones más usadas.

Se continuo con el proceso de caracterización y para poder obtener más detalles al respecto, se revisaron y dividieron las variantes ya encontradas a través de una matriz de afectación (tabla 5). esto con el fin de obtener el malware que causa mayor afectación y poderlo utilizar para la infección y posterior detección y clasificación, y así trabajar en el ambiente controlado con la muestra más representativa de malware ya que es un riesgo el manejo de varias variables de Malware Bancario por su manejo y contención.

Como consideración a los reportes de las diferentes casas Antivirus se realiza una recopilación y clasificación de las variantes dándole una categoría de Alta, Media o Baja según la afectación que representa en el Móvil, con la siguiente definición:

Alta: Roba los usuarios y contraseña de aplicaciones bancarias, se envían a un servidor de C&C, se ejecuta en segundo plano, obtiene permisos full de segundas claves y autenticadores como Google authenticator, para realizar transacciones fraudulentas Difícil de detectar, controlar remotamente los dispositivos móviles, capturas de pantalla, superposición de una pantalla por encima de la interfaz original, haciéndose pasar por la entidad sin que el usuario se percate de ello.

Media: Roba los usuarios y contraseña, se envían a un servidor de C&C tomando algún control, se ejecuta en segundo plano, se vende la información como base de datos a terceros.

Baja: se envían a un servidor de C&C, información del móvil, pero no logra tomar credenciales de las aplicaciones bancarias, se ejecuta en segundo plano, se vende la información como base de datos a terceros.

En la tabla 5 se organiza según la afectación del dispositivo basado en porcentajes de estas infecciones.

NOMBRE VARIANTE	VERSION ANDROID QUE AFECTA	NIVEL DE AFECTACION	PORCENTAJE DE DISPOSITIVOS AFECTADOS	Cantidad de dispositivos Afectados Según la suma de las 2 versión 8 y 9
Indica el nombre de la Variante	Versión de Android que afecta la variante	Indica el nivel de afectación según tabla siguiente	Este es el número de dispositivos afectados que se obtiene del (Total Dispositivos en el mundo, dividido/por Dispositivos	Este total de obtiene de los dispositivos afectado sen cada versión sumadas las dos usadas en este trabajo de grado. Total, de dispositivos afectados por el Malware

			Infectados) x100	

Tabla 5. Clasificación de amenazas dispositivos móviles Android según su compromiso. Construcción propia.

Para la anterior clasificación se dio prioridad a las amenazas más representativas en el mercado con afectación directa a dispositivos Android, que se distribuyan de forma rápida y que su afectación sea alta, así mismo que la cantidad de dispositivos afectados sea considerablemente mayor a la media del mercado de dicha distribución Android en comparación con otras amenazas también la afectación al dispositivo, como lo es perdida de información, cifrado de datos, lentitud de procesador y memoria, y reenvió de la amenaza a otros dispositivos.

Los cuales en su diversidad y objetivo muchos son comunes en su funcionamiento, basados en servidores C&C (Comando y Control).

Resultado actividad 3 fase 1

De las tablas anteriores obtenemos como resultado la siguiente (tabla 6) según el número de dispositivos afectados:

NOMBRE VARIANTE	VERSION ANDROID QUE AFECTA	NIVEL DE AFECTACION	PORCENTAJE DE DISPOSITIVOS AFECTADOS	Cantidad de dispositivos Afectados Según la suma de las 2 versión 8 y 9
Cerberus	V 8.0 y 9.0	Alta	18%	236.610
Alien	V 8.0 y 9.0	Alta	15%	197.175
teatv.apk	V 8.0 y 9.0	Alta	12%	157.740
BlackRock	V 8.0 y 9.0	Alta	10%	131.450
Gustuff	V 8.0 y 9.0	Alta	10%	131.450
Hydra	V 8.0 y 9.0	Alta	8%	105.160
Gravity RAT	V 8.0 y 9.0	Media	7%	92.015

Anubis Bankbot.	V 8.0 y 9.0	Media	7%	92.015
Ginp	V 8.0 y 9.0	Media	7%	92.015
Mispadu	V 8.0 y 9.0	Media	7%	92.015
Anubis	V 8.0 y 9.0	Media	6%	78.870
Eventbot	V 8.0 y 9.0	Baja	4%	52.580

Tabla 6. Resultado de la clasificación de los dispositivos afectados por Malware según el porcentaje de uso y distribución en el mercado. Fuente propia a partir de lo identificado y las fuentes de consulta.

De acuerdo a la cantidad de dispositivos en el mundo [50], se tiene que el porcentaje de dispositivos afectados de donde salen los resultados del Total dispositivos Android en su versión 8.0 + 9.0 es de 1314.5 Millones de Dispositivos, los cuales se toman de la Tabla 3. de acuerdo al registro hasta el 2020.

Después de su clasificación en la tabla 6 y para efectos prácticos, se tomaron los 6 que más afectan los dispositivos móviles de tipo Android en sus últimas dos versiones más usadas los cuales son:

IoC_Cerberus

IoC teatv.apk

IoC alien

IoC _Gustuff

IoC_Hydra

IoC_BlackRock

También se muestra el resultado de la clasificación de la posible afectación según el comportamiento del malware dentro del dispositivo móvil. A continuación, se muestra la funcionalidad y permisos del malware bancario, lo que incluye las siguientes capacidades:

- Control remoto, usando varios métodos de comunicación con el servidor C&C

- Obtención de información del dispositivo
- Descarga y ejecución de aplicaciones adicionales
- Superposición de aplicaciones legítimas y específicas con pantallas de phishing, usando varios técnicos
- Recolectar las credenciales ingresadas en los formularios de phishing y enviarlas al servidor C&C encriptadas no encriptadas
- Interceptar, redirigir, enviar y eliminar mensajes SMS, para evitar la autenticación de dos factores basada en SMS Dependiendo de los permisos obtenidos durante y después de la instalación, sofisticado Los troyanos bancarios que se dirigen a la plataforma Android también suelen ser capaces de:
- Mostrar notificaciones falsas para indicar a las víctimas que inicien las aplicaciones bancarias específicas
- Obtener la lista de aplicaciones en ejecución
- Obtener y editar la lista de contactos
- Obtener el registro de llamadas telefónicas, hacer y redirigir el teléfono llamadas
- Acceder al almacenamiento del dispositivo
- Abrir un navegador y navegar a sitios web específicos
- Acceder a la cámara
- Comenzar en el inicio del dispositivo
- Bloquear y desbloquear de forma remota el dispositivo mediante el establecimiento de una contraseña de pantalla de bloqueo de la elección de los atacantes
- Mostrar actividad en pantalla completa para cubrir la actividad maliciosa en ejecución en segundo plano
- Grabación de un video de la pantalla
- Registro de teclas
- Ejecución como proxy para enrutar el tráfico de red a través del dispositivo móvil comprometido para engañar a los mecanismos de detección de fraude de los bancos

Una vez clasificadas se rotularon como posibles malware a controlar, considerando igualmente, si las cepas o códigos fuentes pueden conseguirse para las pruebas respectivas, así mismo de la tabla 6, se tomó la muestra con mayor afectación a número de dispositivos de igual manera en esta actividad se obtuvo 1 sepa del malware bancario de nombre CERBERUS la cual es la que afecta la mayor cantidad de dispositivos en las versiones 8 y 9 un total de 236.610 para ser probado en el ambiente controlado.

La sepa se buscó y descargo para ser usada en el ambiente controlado de los distintos repositorios los cuales se referencian en la tabla 7:

Resultado Actividad 4 fase 1

Listado de repositorios

WEB	OBSERVACIONES
ANY.run	Gratis, requiere registro
Contagio Malware Dump	Gratis, requiere registro
Das Malwerk	Gratuito
FreeTrojanBotnet	Gratis, requiere registro
KernelMode.info	Gratis, requiere registro
MalShare	Gratis, requiere registro
Malware.lu's AVCaesar	Gratis, requiere registro
MalwareBlacklist	Gratis, requiere registro
Malware DB (The Zoo)	Gratuito
MalwareDomainList	Gratis, requiere registro
Malwareurls	Gratis, requiere registro
Malwr	Gratis, requiere registro

Open Malware	Gratuito
Objective-See Collection	Gratuito, malware para Mac
PacketTotal	Gratuito (archivos pcacp)
Sndbox	Gratuito
URLhaus	Gratuito (sitios vivos)
VirusBay	Gratis, requiere registro
Virusign	Gratis, requiere registro
VeriSign	Gratis, requiere registro, incluye muestras Android
VirusShare	Gratuito
VxVault	Gratuito

Tabla 7. repositorios de Malware consultados para ser descargado para intenciones prácticas de esta tesis de grado.

2.1.4 Caracterización de los IOC para dispositivos móviles Android versiones 8 y 9

Una vez identificadas las versiones Android y los diferentes malware que puedan afectar a los Smartphone, se continua con la caracterización de los IoC que puedan ser usados en la identificación de una de las sepas.

Para el desarrollo de esta actividad, se analizaron diferentes fuentes o repositorios de IOC para extraer de ellos los más representativos y mejor ranqueados para el análisis de Malware en dispositivos Móviles Android en sus últimas dos versiones. En esta actividad se clasificaron los Indicadores de Compromiso para Android con las amenazas Ramsonware y Malware que más los afecta para así definir de manera clara cuales de estos se cargarán en la herramienta semiautomatizada para la detección, clasificación y contención del código malicioso.

Los repositorios gratuitos que se revisaran durante el desarrollo de esta investigación son IOC Bucket y Openioc, ambos publicados bajo licencia Apache 2. Así mismo se considerara la construcción propia de un repositorio local con las variantes que se trabajaran en el laboratorio controlado, como lo hace el Gobierno de España en cabeza del centro criptológico nacional ha creado una completa guía de Indicadores de compromiso nombrada (CCN-STIC-423) que consiste en un completo compendio de técnicas y aplicación de los indicadores de compromiso para la defensa nacional basándose en la aplicación de técnicas forenses avanzadas que permitan la detección de potenciales amenazas, aunque estas no son en tiempo real, lo que conlleva a una vulnerabilidad de repeler el ataque en el instante que sucede.

Las diferentes bases de datos con información consultadas fueron:

- https://www.incibe-cert.es
- https://github.com/eset/malware-ioc
- https://www.welivesecurity.com
- https://www.kaspersky.es
- https://www.fireeye.com
- IOC Bucket y Openioc
- https://blog.malwarebytes.com/glossary/ioc/https://threatfox.abuse.ch/browse/
- https://github.com/DoctorWebLtd/malware-iocs

Dentro de la investigación realizada se definieron unas características que deben tener los IoC, basado en los estándares y normas de estos, que sirvan de base en la construcción de indicadores de compromiso para Android para ser usados y cargados en la aplicación semiautomatizada que se construyó, dichas características se pueden observar en la tabla 8.

Al frente de cada campo se da la explicación de lo que contiene.

Atributos de los Archivos	nombre, md5 o sha1, tamaño, fecha de compilación, funciones exportadas o importadas, nombres de las secciones.
Nombre del Malware	Nombre del Malware
hash del Archivo de entrada Mde5	Firma que identifica el Malware en las diferentes plataformas antivirus
Autor	Creador del Malware
Fecha Creado	Creación del malware
Fecha Modificado	Última modificación realizada al malware
Descripción	Descripción del malware
Tamaño	Tamaño del archivo de infección del malware
Acciones del malware sobre el sistema	Acciones que realiza el malware sobre el dispositivo
Servicios Red	Servicios de red que usa el malware, sitios de conexión
Procesos realizados en el sistema	Procesos que realiza el malware en el sistema
Versión sistema:	Versión del sistema afectado
Archivos	Archivos que afecta el malware
Fecha y Hora Ultima Ejecución	Fecha y hora de la última ejecución del malware

Tabla 8. Caracterización de un Indicador de Compromiso para Android por cada Malware o Ramsonware identificado en la tabla anterior. (Construcción Propia.)

Posterior a tener la información o resultado, se procede a construir para la lectura y transferencia de datos a otras aplicaciones en este caso a la herramienta semiautomatizada, esta caracterización se debe realizar para cada amenaza escogida. Después de obtenido los resultados de la tabla estos se llevan a XML, lenguaje simple para la lectura en la herramienta semiautomatizada.

Como resultado de la anterior tabla se muestra la Construcción de 6 IoC en XML de cada uno de los indicadores según las amenazas clasificadas.

Como resultado de esta actividad fase 1 obtenemos:

Indicador de Compromiso para el malware Cerberus:

Nombre IoC	IoC_Cerberus
Nombre del Malware	Cerberus
hash del Archivo de entrada Mde5	84da367dd962210f27858799fe25d79f
Autor	Desconocido
Fecha Creado	2021-09-16 19:17:05
Fecha Modificado	2021-09-17 02:29:54
Descripción	el malware es capaz de detectar cuando una aplicación es iniciada por parte del usuario, y de esta forma mostrar una ventana falsa solicitando las credenciales de acceso a la entidad bancaria.
Tamaño	909.80 KB
Acciones del malware sobre el sistema	android.permission.READ_PHONE_STATE android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.CALL_PHONE

	android.permission.RECORD_AUDIO android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.REQUEST_DELETE_PACKAGES android.permission.READ_EXTERNAL_STORAGE android.permission.RECEIVE_BOOT_COMPLETED android.permission.USE_FULL_SCREEN_INTENT android.permission.ACCESS_NETWORK_STATE android.permission.WAKE_LOCK android.permission.FOREGROUND_SERVICE android.permission.GET_ACCOUNTS
Servicios Red	com.google.android.webview.org.chromium.content.app.SandboxedProcessService0 - {"org.chromium.base.process_launcher.extra.bind_to_caller":"true", "org.chromium.content.common.child_service_params.library_process_type":"4"}
Procesos realizados en el sistema	Files Opened /data/user/0/com.djmaoevlgk.echnsw/shared_prefs/ring0.xml Files Written /data/user/0/com.djmaoevlgk.echnsw/shared_prefs/ring0.xml Files Deleted /data/user/0/com.djmaoevlgk.echnsw/shared_prefs/ring0.xml.bak

	Files Copied /data/user/0/com.djmaoevlgk.echnsw/shared_prefs/ring0.xml Services Opened telephony_subscription_service phone alarm activity window keyguard device_policy appops connectivity display user autofill power input_method layout_inflater jobscheduler
Versión sistema:	Todas las Versiones de Android incluidas las 8.0 y 9.0
Archivos	Google_Play_Store.apk
Fecha y Hora Ultima Ejecución	2021-09-16 19:17:05

Indicador de Compromiso para teatv.apk:

Nombre IoC	IoC teatv.apk
Nombre del Malware	teatv.apk
hash del Archivo de entrada Mde5	d4420465fced7188fa28d8ed934a96af
Autor	Desconocido
Fecha Creado	2021-01-06 22:10:36
Fecha Modificado	2021-01-06 22:15:12
Descripción	El malware instala un servicio de accesibilidad en el teléfono para controlar toda la actividad del mismo, con el fin de detectar la apertura de aplicaciones bancarias
Tamaño	3.20 MB (3354715 bytes)
Acciones del malware sobre el sistema	android.permission.INTERNET android.permission.SYSTEM_ALERT_WINDOW android.permission.WRITE_SMS android.permission.RECEIVE_MMS android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.READ_PHONE_STATE android.permission.READ_SMS

	android.permission.USE_BIOMETRIC android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.QUERY_ALL_PACKAGES android.permission.READ_SYNC_SETTINGS android.permission.USE_FULL_SCREEN_INTENT android.permission.REQUEST_PASSWORD_COMPLEXITY android.permission.WAKE_LOCK android.permission.REORDER_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.FOREGROUND_SERVICE android.permission.REQUEST_DELETE_PACKAGES android.permission.GET_ACCOUNTS
Servicios Red	http[://batroslunk.top:80/api/ http[://gaweawgeaweg232.top:80/api/ 45.14.50.74:80 http://batroslunk.top/api/botupdate http://batroslunk.top/api/getbotinjects http://batroslunk.top/api/getkeyloggers http://batroslunk.top/api/botupdate http://batroslunk.top/api/botupdate
Procesos realizados	android.intent.action.RESPOND_VIA_MESSAGE android.accessibilityservice.AccessibilityService

en el sistema	android.intent.action.MAIN android.intent.action.SEND android.intent.action.SENDTO android.provider.Telephony.WAP_PUSH_DELIVER android.intent.action.BOOT_COMPLETED android.intent.action.QUICKBOOT_POWERON com.htc.intent.action.QUICKBOOT_POWERON android.intent.action.USER_PRESENT android.intent.action.PACKAGE_ADDED android.intent.action.PACKAGE_REMOVED android.intent.action.ACTION_PACKAGE_ADDED android.provider.Telephony.SMS_RECEIVED android.provider.Telephony.SMS_DELIVER
Versión sistema:	Todas las Versiones de Android incluidas las 8.0 y 9.0
Archivos	Android Type APK Package Name heart.vacant. choice Main .RenamedClass9 Internal Version 1 Displayed Version 1.0 Minimum SDK Version 24 Target SDK Versión 30
Fecha y Hora Ultima Ejecución	2021-01-07 12:15:07

Indicador de Compromiso para Alien:

Nombre IoC	IoC alien
Nombre del Malware	Alien, Coronavirus
hash del Archivo de entrada Mde5	b8328a55e1c340c1b4c7ca622ad79649
Autor	Desconocido
Fecha Creado	2020-02-07 18:13:36
Fecha Modificado	2020-02-07 18:13:36
Descripción	Malware Bancario que roba contraseñas de más de 200 aplicaciones de Android, entre ellas algunas como WhatsApp o Instagram. es un troyano bancario Android relativamente nuevo y apenas conocido, que puede acceder de forma remota, robar los SMS y otras notificaciones y recopilar nuestra lista de contactos.
Tamaño	1.55 MB (1621042 bytes)
Acciones del malware sobre el sistema	Registro de teclas pulsadas (keylogger). Instalación de otras aplicaciones. Desvío de llamada. Acceso a los datos de localización. Robo de agenda de contactos.
Servicios Red	iba.jkgmnr.nomttdnemcorujdfjfsfsmrb.zebkhdikijpr iba.jkgmnr.nomttdnemcorujdfjfsfsmrb.lzfsrglmmlww iba.jkgmnr.nomttdnemcorujdfjfsfsmrb.rtlcquhyc

Procesos realizados en el sistema	android.permission.SEND_SMS android.permission.READ_CONTACTS android.permission.CALL_PHONE android.permission.RECEIVE_SMS android.permission.READ_PHONE_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_SMS android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.READ_EXTERNAL_STORAGE android.permission.RECEIVE_BOOT_COMPLETED android.permission.USE_FULL_SCREEN_INTENT android.permission.ACCESS_NOTIFICATION_POLICY android.permission.READ_SYNC_STATS android.permission.ACCESS_NETWORK_STATE android.permission.WAKE_LOCK android.permission.FOREGROUND_SERVICE android.permission.GET_ACCOUNTS
Versión sistema:	Desde la versión Android 4.0.3, 4.0.4 incluidas las 8.0 y 9.0.
Archivos	Files Opened /data/data/hdjro.nzaqrgffealnhmorwihd.mfukiybfx/app_DynamicOptDex/ZE.json Files Written

	/data/data/hdjro.nzaqrgffealnhmorwihd.mfukiybfx/app_DynamicOptDex/ZE.json
Fecha y Hora Ultima Ejecución	2020-08-20 11:24:16

Indicador de Compromiso para Gustuff:

Nombre IoC	IoC _Gustuff
Nombre del Malware	Gustuff
hash del Archivo de entrada Mde5	a83681bd8c84907dba772fe8feb0ca0d
Autor	Desconocido
Fecha Creado	2019-03-13 21:41:51
Fecha Modificado	2021-07-09 21:35:22
Descripción	infecta a las víctimas con un mensaje de texto y las engaña para que proporcionen acceso a la función de accesibilidad de Android. Ese servicio permite a los teléfonos Android tomar medidas de forma predeterminada, como aumentar el tamaño de un icono o leer texto en voz alta. Una vez dentro, Gustuff puede desviar fondos del software de pago llamado Servicio de transferencia automática.
Tamaño	1.13 MB (1186716 bytes)
Acciones del malware sobre el sistema	android.permission.READ_PHONE_STATE android.permission.READ_CONTACTS android.permission.CALL_PHONE android.permission.RECEIVE_SMS

	android.permission.SEND_SMS android.permission.READ_SMS android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE
Servicios Red	hxxp://88.99.227[.]26/html2/2018/GrafKey/new-inj-135-3-dark.html hxxp://88.99.227[.]26/html2/arc92/au483x.zip hxxp://94.130.106[.]117:8080/api/v1/report/records.php hxxp://88.99.227[.]26/html2/new-inj-135-3-white.html hxxp://facebook-photos-au[.]su/ChristinaMorrow hxxp://homevideo2-12l[.]ml/mms3/download_3.php Facebook-photos-au.su Homevideo2-12l.ml videohosting1-5j.gq
Procesos realizados en el sistema	Envió de Mensajes de Texto Robo de credenciales de inicio de apps Bancarias Robo de contactos y reenvió de los mismos Permisos full a la aplicación maliciosa
Versión sistema:	Desde la Versión 8 en delante de Android
Archivos	classes.dex Trojan/Android.Marcher.50497 ANDROID/Spy.Banker.YD.Gen SMS Libreta de direcciones

Fecha y Hora Ultima Ejecución	2021-07-09 21:35:22

Indicador de Compromiso para Hydra:

Nombre IoC	IoC_Hydra
Nombre del Malware	Hydra
hash del Archivo de entrada Mde5	0962f16cc5031010c7ed6b9f456ec4fe
Autor	Desconocidos
Fecha Creado	2021-09-24 20:16:38
Fecha Modificado	2021-10-07 06:54:11
Descripción	Hydra es otra variante de Android Bankbot. Utiliza superposición para robar información como Anubis. Su nombre proviene de panel de mando y control. De julio de 2018 a marzo de 2019, hubo al menos 8-10 muestras en Google Play Store.
Tamaño	8.65 MB (9069403 bytes)
Acciones del malware sobre el sistema	android.permission.DISABLE_KEYGUARD android.permission.INTERNET android.permission.SEND_SMS android.permission.WRITE_SMS android.permission.WRITE_EXTERNAL_STORAGE android.permission.CALL_PHONE android.permission.READ_SMS android.permission.SYSTEM_ALERT_WINDOW

	android.permission.CHANGE_WIFI_STATE android.permission.RECEIVE_SMS android.permission.READ_CONTACTS
Servicios Red	com.google.android.finsky.services.ContentSyncService (com.android.vending) com.google.android.gms.app.service.PackageBroadcastService (com.google.android.gms) com.google.android.gms.games.service.GamesIntentService (com.google.android.gms) com.google.android.gms.people.service.bg.PeopleBackgroundTasks (com.google.android.gms) com.google.android.gms.icing.service.IndexWorkerService (com.google.android.gms) com.google.android.partnersetup.RlzPingIntentService (com.google.android.partnersetup)
Procesos realizados en el sistema	Files Opened /data/app/com.qcavvlvk.woucngh-1.apk /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/eomzbmcr.xjjg /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1662631072.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/com.qcavvlvk.woucngh-1.apk.eirkapk1.gxs /data/data/com.qcavvlvk.woucngh/shared_prefs/multidex.version.xml /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk1838307626.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1470938581.gxs

	/data/data/com.qcavvlvk.woucngh/shared_prefs/multidex.version .xml.bak /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1947353772.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk608350.gxs Files Written /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1662631072.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk1838307626.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1470938581.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1947353772.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk608350.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk1380775963.gxs Files Deleted /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1662631072.gxs /data/data/com.qcavvlvk.woucngh/shared_prefs/multidex.version .xml.bak /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa /eomzbmcr.xjjg

	/data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/com.qcavvlvk.woucngh-1.apk.eirkapk1.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk1838307626.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1470938581.gxs /data/data/com.qcavvlvk.woucngh/shared_prefs/multidex.version.xml /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1947353772.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk608350.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk1380775963.gxs Files Copied /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1662631072.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk1838307626.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1470938581.gxs /data/data/com.qcavvlvk.woucngh/shared_prefs/multidex.version.xml /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk-1947353772.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk608350.gxs /data/data/com.qcavvlvk.woucngh/bicjxnddha/nqcuwzxjvqhqmpa/tmp-com.qcavvlvk.woucngh-1.apk.eirkapk1380775963.gxs

	Files Dropped 65744c3b869562b40459361972fc169cbb11920ecb04cdeceabfa61fbed24f74
Versión sistema:	Desde la Versión 8 en delante de Android
Archivos	android.accessibilityservice.AccessibilityService android.intent.action.RESPOND_VIA_MESSAGE android.intent.action.MAIN android.intent.action.SENDTO android.intent.action.SEND android.intent.action.BOOT_COMPLETED android.provider.Telephony.WAP_PUSH_DELIVER android.app.action.DEVICE_ADMIN_ENABLED android.provider.Telephony.SMS_DELIVER android.intent.action.PACKAGE_REMOVED
Fecha y Hora Ultima Ejecución	2021-10-04 06:51:07

Indicador de Compromiso para BlackRock:

Nombre IoC	IoC_BlackRock
Nombre del Malware	BlackRock
hash del Archivo de entrada Mde5	36cd2ea94bcf9f9a9959dc4c1c489933

Autor	LokiBot malware family
Fecha Creado	2020-06-27 11:25:16
Fecha Modificado	2020-06-23 17:23:02
Descripción	BlackRock, que se encarga de extraer contraseñas y datos de tarjetas bancarias.
Tamaño	1.81 MB (1896652 bytes)
Acciones del malware sobre el sistema	android.permission.WRITE_CONTACTS android.permission.READ_PHONE_STATE android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_CONTACTS android.permission.READ_SMS
Red	Hosts: 172.217.23.110 216.58.207.42 176.121.14.127 172.217.21.195
Procesos y servicios	Files Opened /data/data/ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplb/app_DynamicOptDex/DP.json Files Written /data/data/ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplb/app_DynamicOptDex/DP.json Process And Service Actions Processes Tree 8145 - zygote 15529 - ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplb

	15619 - ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplb 15657 - ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplb:cproc
Versión del sistema:	Versiones Android a partir de la 4.0
Archivos	ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Ospynaive ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.MainActivity true ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Weagerchronic ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Uarrivedecline ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Uleafframe ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Smsmnd.SendSms ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Ecraterimitate ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Ideallabor ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Tblamereunion ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Psuddenlobster ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Uusefulurge

	ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Iwhatmelt ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Ppresentdove ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Sradarover ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Permission ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Nscrubepisode ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Maccidentbase ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.InjectCC ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Hyarddespair ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Inject ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Lsupremecurve ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Dhometwin ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Jsisterusual ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Hfrosttourist ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Dcastleamateur ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Admin

	ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Zspatialtrade ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Systems ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Zreopencharge ayxzygxgagiqhdnjnfduerzbeh.hme.egybgkeziplbzsohzecuojrzhqxqmkartys.brbgrdmutfqe.Qquicksection
Fecha y Hora Ultima Ejecución	2020-06-23 17:23:02

Tablas 9. Resultado de la caracterización de los Indicadores de compromiso, para las 6 principales afectaciones tipo malware Bancario a dispositivos Android en sus dos versiones más usadas.

Como resultado de los anteriores IOC se toma para este trabajo de grado el construido para CERBERUS el cual será objeto de estudio y utilización en el ambiente controlado.

2.1.5 IOC para dispositivos móviles Android Versiones 8 y 9.

Con base en los resultados anteriores, se hizo la construcción del IoC que apliquen en las últimas 2 versiones de Android más usadas y como se indicó, aplica para la versión 8 y 9, obteniendo un listado de dichos IoC que puedan ser usados. Esta construcción consideró temas como la posible obtención del código fuente, usabilidad, que sea *free* o que se pueda usar para efectos académicos.

NOMBRE IOC	HASH MALWARE IDENTIFICADO	REPOSITORIO
Nombre del indicador de compromiso para su identificación en la herramienta	Esta es la firma para identificar el Malware, tomado de la búsqueda realizada para	Donde se ubica el Indicador de compromiso

	cada uno en virus Total	

Tabla 10. IOC construidos para Dispositivos Móviles Android en sus últimas dos versiones. (construcción Propia).

Resultados obtenidos en la fase 1:

A continuación (tabla 10) se tienen los resultados consolidados de los Indicadores de compromisos Identificados para ser construidos en el XML, los cuales consumirá en la herramienta semiautomatizada.

NOMBRE IOC	HASH MALWARE IDENTIFICADO	REPOSITORIO
IoC_Cerberus	84da367dd962210f27858799fe25d79f	Local / Propio
IoC teatv.apk	d4420465fced7188fa28d8ed934a96af	Local / Propio
IoC alien	b8328a55e1c340c1b4c7ca622ad79649	Local / Propio
IoC _Gustuff	a83681bd8c84907dba772fe8feb0ca0d	Local / Propio
IoC_Hydra	0962f16cc5031010c7ed6b9f456ec4fe	Local / Propio
IoC_BlackRock	36cd2ea94bcf9f9a9959dc4c1c489933	Local / Propio

Tabla 11. Resultado IOC que se construyeron como XML para consumir desde la aplicación semiautomatizada.

Con las fases anteriores, se logra el primer objetivo específico que es la caracterización de los diferentes IoC (6 en total) que puedan aplicar a las 2 últimas versiones más usadas de Android, partiendo de la misma identificación del malware y las versiones Android.

2.2 Fase 2: Propuesta de un mecanismo de clasificación de amenazas para dispositivos móviles Android en sus últimas dos versiones.

A continuación, se presentó la propuesta de clasificación de amenazas de tipo Malware Bancario según su afectación, propagación, y dificulta de detección y contención, dado que

de esta manera es mal fácil identificar cual es la que causa una mayor afectación y al conocerla se puede detectar y clasificar para efectos de esta tesis, obteniendo así la información necesaria para poder ejecutar el laboratorio, en los dispositivos Móviles Android de acuerdo al nivel de impacto en el dispositivo, para lo cual, se definieron los siguientes parámetros (tabla 12):

Nivel: Según el número de características seleccionadas se da el nivel de bajo medio o alto.

Características: estas son las que tiene en común en su funcionalidad o afectación un malware

Características Seleccionadas: Numero de características seleccionadas llevado a porcentaje

Así mismo, los niveles de clasificación se miden según el porcentaje de características que aplican a ese malware en la versión Android, a saber (tabla 12:

Bajo: cuando tiene 1 o 2 características del Malware aplicado a la Versión Android

Medio: cuando tiene entre 3 y 5 características del Malware aplicado a la versión Android

Alto: Cuando tiene entre 6 y 8 características del Malware aplicado a la versión Android

Nivel	% Características	Características Seleccionadas
Bajo	0% a 33%	1-2
Medio	34% a 66%	3-5
Alto	67% a 100%	6-8

Tabla 12. de Clasificación de amenazas según nivel y características seleccionadas.

Para la selección del tipo de comportamiento de cada Malware, se consideraron 8 tipos de acciones que se podrían ejecutar en un dispositivo si es infectado, que son (tabla 13):

1 Registro de teclas pulsadas
2 Captura de formularios
3 Capturas de pantalla y grabación de video
4 Inyección de campos de formulario fraudulentos
5 Inyección de páginas fraudulentas
6 Redirección de páginas bancarias
7 Registro de teclas pulsadas
8 Hombre-en-el-medio (man-in-the-middle)

Para lo cual, se tomó cada Malware y se validó de acuerdo a la característica del mismo, el tipo de comportamiento, tabulando los datos en la siguiente tabla 13, fijando una “x” de acuerdo a la aplicabilidad:

Malware: Nombre del Malware

Posibles Comportamientos: Comportamientos según cada característica, asignándole un número (acorde a la descripción anterior).

MALWARE	**POSIBLES COMPORTAMIENTOS**								
Comportamiento	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Total**

Tabla 13. Clasificación Malware tipo bancario Construcción propia

El siguiente modelo de clasificación del Malware Tipo Bancario es el resultado que se realiza con base a su comportamiento común al infectar un teléfono móvil.

Dado lo anterior y en consideración de los diferentes comportamientos, se diligencia la siguiente tabla, la cual fue tomada y ajustada de [51]:

Resultados obtenidos en la fase 2:

Tabla de Clasificación del malware tipo bancario según su comportamiento:

MALWARE	POSIBLES COMPORTAMIENTOS								
Comportamiento	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Total**
Cerberus	**X**	**X**	**X**	**X**		**X**	**X**	**X**	**7**
teatv.apk	**X**		**X**		**X**	**X**	**X**		**5**
alien	**X**	**X**	**X**			**X**	**X**		**5**
Gustuff	**X**	**X**	**X**			**X**	**X**		**5**
Hydra	**X**	**X**	**X**			**X**	**X**		**5**
BlackRock	**X**	**X**	**X**	**X**		**X**	**X**		**6**

Tabla 14. Clasificación Malware tipo bancario, construida con base al formato de la clasificación de familias Ransomware, revista UIS Ingenierías “Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware” [51]

Resultados obtenidos en la fase 2:

Esta es una clasificación de los posibles impactos (columna “nivel” de la tabla 15) que pueda generar un tipo de malware, construcción apoyada por la clasificación de familias realizada en [51] y ajustada a este trabajo de grado.

MALWARE	NIVEL	DETECCION	CALIFICACIÓN	PORCENTAJE
Cerberus	Alta	IoC_Cerberus	7	90%
teatv.apk	Media	IoC teatv.apk	5	66%

alien	Media	IoC alien	5	66%
Gustuff	Media	IoC _Gustuff	5	66%
Hydra	Media	IoC_Hydra	5	66%
BlackRock	Alta	IoC_BlackRock	6	75%

Tabla 15. Resultado clasificación Malware Tipo Bancario Resumen. (construcción propia).

De la anterior tabla 15, se puede observar el valor y utilidad dado que con la clasificación se obtiene que el malware más representativo, que para el caso es CERBERUS, así como valores de referencias de otros malwares potencialmente dañinos, como es el caso de BlackRock (con un 75%). En consideración de la prueba de concepto a realizar, se tomó el porcentaje más alto (Cerberus)) y con el cual se hizo las pruebas controladas de infección para lograr su detección y clasificación.

2.3 Fase 3: Diseño de una aplicación que, de forma semiautomatizada, detecte y clasifique posible Malware en el dispositivo Android versión 8 y 9

En esta fase se realizó el diseño y construcción de una aplicación semiautomatizada la cual será la encargada de cargar los IOC construidos para Android, así como la encargada de ejecutarse en el teléfono para la detección del Malware de tipo bancario. Esto se llevó a cabo a través de las siguientes actividades:

- Levantamiento de Requisitos para la herramienta Semiautomatizada
- Posibles controles basado en la herramienta Semiautomatizada para Android en las versiones 8 y 9.
- Creación del código fuente utilizado para la herramienta semiautomatizada usada en Android.

  Pruebas de funcionamiento de la herramienta semiautomatizada en emulador Android

2.3.1 Levantamiento de Requisitos para la herramienta Semiautomatizada.

En esta actividad, se realizó una elicitación de requisitos para la construcción de la herramienta semiautomatizada.

Por lo cual, para dicho levantamiento de la Información se usó la técnica estandarizada de E-licitación de requisitos, que es el estándar más importante y más ampliamente reconocido para la especificación, diagramación y documentación de software de calidad, con el propósito de identificar problemas y oportunidades de mejora, por medio de la e licitación de requisitos, se realizó el afinamiento del desarrollo ya que este permite, de una manera clara y eficiente lo que realmente requiere el sistema para poder operar correctamente.

A continuación, se presenta el formato usado para ello:

FORMATO DE ELICITACIÓN DE REQUISITOS DE SOFTWARE

Información del Proyecto Herramienta Semiautomatizada para Android	
PROYECTO	"Nombre del proyecto"

HERRAMIENTA SEMIAUTOMATIZADA ANDROID
PRESENTACIÓN
Breve resumen de la funcionalidad de la herramienta
PROBLEMA, NECESIDAD, OPORTUNIDAD A RESOLVER
Problema a resolver con el desarrollo de la herramienta
OBJETIVOS
Objetivos que se pretenden abarcar con la herramienta

ALCANCE
Hasta donde se pretende llegar con la herramienta que hará en el sistema Android, como lo hará
REQUISITOS FUNCIONALES (FR)
La descripción de los requisitos se redacta en lenguaje natural, sencillo y se puede complementar con gráficos, fórmulas, etc. En lo posible evitar el uso de siglas, abreviaturas, tecnicismos **Definen en un lenguaje natural, propio del entorno del usuario, las funciones que éste desea del sistema. Se recomienda utilizar una entrada en el Glosario para cada término o expresión que pueda no tener un significado único.** **Cada clase de requisito se registra en una estructura tabular con al menos 3 columnas:** **Número de secuencia del requisito** **Descripción en lenguaje natural del requisito (no en términos de la solución informática)** **Observaciones:**

ESPECIFICACIÓN DE REQUISITOS DEL SISTEMA SEMIAUTOMATIZADO		
REQUISITOS FUNCIONALES DEL MODULO SEMIAUTOMATIZADO		
#	**Descripción del requisito**	**Observaciones**
1		
2		
N		

GLOSARIO
Palabras clave usadas
ANEXOS

DESCRIPCIÓN DE LOS GRUPOS USUARIOS DEL SISTEMA

Que usuarios usaran el sistema el propietario usuario estándar, root, administrador.

REQUISITOS NO FUNCIONALES (NFR)

Esta clase de requisitos define atributos o cualidades generales del sistema resultante; establece restricciones sobre el producto que está siendo desarrollado y el proceso de desarrollo, además, especifica restricciones externas que debe cumplir el producto.

Por ejemplo: requisitos de seguridad, de interface, operacionales, de facilidad de uso, de confiabilidad, de rendimiento, de aceptación, de portabilidad, de documentación, de recursos. En particular puede describirse la carga esperada que pueda tener el sistema en términos de usuarios simultáneos conectados, horarios de uso, estaciones de trabajo, transacciones por unidad de tiempo, volumen de registros u objetos a almacenar, controles de acceso.

A juicio del analista y según aplica para un módulo o componente en particular, se pueden adicionar las dos siguientes categorías complementarias de requisitos, las cuáles deben guardar concordancia directa con los requisitos funcionales y no funcionales.

REQUISITOS ESPECIFICOS DE INFORMACIÓN

que requerimientos en específico se requieren para que la aplicación funcione correctamente, procesos del sistema carga de archivos etc.

REQUISITOS EXCLUIDOS

Se refiere a las reglas o limitaciones que debe cumplir la solución.

REQUISITOS DE RESTRICCIÓN

El texto presentado no puede ocupar más de una línea

1	
2	
3	

4	

Tabla 16. Formato E-licitación de requisitos (construcción propia).

Resultados obtenidos en la fase 3:

A continuación, se expone el resultado de la e-licitación de requisitos con la cual se pretende dar una acertada explicación del funcionamiento y funcionalidades de la herramienta para Android.

ELICITACIÓN DE REQUISITOS DE SOFTWARE

Información del Proyecto Herramienta Semiautomatizada para Android	
PROYECTO	Herramienta semiautomatizada para Android Versiones 8 OREO y 9 PIE

HERRAMIENTA SEMIAUTOMATIZADA ANDROID
PRESENTACIÓN
Android lleva varios años aprovechando de manera exitosa la tecnología de los Sistemas de Información por lo cual su uso en dispositivos móviles se ha incrementado pero también de esa misma manera se han incrementado los ataques a estos dispositivos por medio de Malware Bancario, ya que nuestras transacciones han migrado de oficinas físicas a las virtuales lo cual aprovechan los atacantes para vulnerar estos, por tal motivo crece la relevancia en la protección de nuestra información por lo cual se ha diseñado una herramienta que cumpla con el objetivo de informar al usuario que su dispositivo está siendo afectado..
PROBLEMA, NECESIDAD, OPORTUNIDAD A RESOLVER
Actualmente se presentan muchas amenazas de tipo malware bancario en dispositivos Android y no hay una herramienta adecuada a parte de los antivirus o detección por firmas para detectar y clasificar a tiempo las amenazas que se presentan en el dispositivo móvil promoviendo o informando de posibles controles a llevar a cabo a los usuarios o propietarios de los móviles.
OBJETIVOS
Detectar y clasificar amenazas de tipo malware bancario en dispositivos Android versiones 8 y 9, y proponer controles a los usuarios.

ALCANCE

Detección y clasificación de amenazas tipo bancario en Android 8 y 9 informando al usuario de una posible infección y proponerle posibles controles.

REQUISITOS FUNCIONALES (FR)

La herramienta desarrollada debe poder ejecutarse en segundo plano,

leer lo recursos del sistema Android así mismo poder obtener permisos tipo root para poder ejecutar acciones en el sistema, adicional cargar un archivo en texto plano o XML, para ser leído por la herramienta el cual contendrá los IoC, una vez toma el estado inicial del dispositivo testeara que no se produzcan cambios en la escritura en disco, memoria, procesador, y recursos que afectan el malware bancario, una vez se produzca un cambio informara a el usuario para tomar acciones, con posibles controles dados por la herramienta como bloquear escritura, quitar permisos a la aplicación, aislar el proceso, desinstalar la aplicación maliciosa o pedir intervención del usuario par otras acciones

Observaciones:

ESPECIFICACIÓN DE REQUISITOS DEL SISTEMA SEMIAUTOMATIZADO		
REQUISITOS FUNCIONALES DEL MODULO SEMIAUTOMATIZADO		
#	**Descripción del requisito**	**Observaciones**
1	**Tomar estado inicial del sistema**	**Realizar una captura del estado del sistema en cuanto permisos, memoria, disco, procesador, aplicaciones instaladas recientemente entre otras.**
2	**Revisar cada x tiempo Memoria, Permisos,**	**La herramienta se ejecutará en segundo plano y cada cierto tiempo verificará algún tipo de modificación en el dispositivo.**
3	**Cargar Archivo XML o texto plano**	**La herramienta debe permitir la carga de archivos xml o texto con los IoC contra malware bancario**

	4	**Revisar aplicaciones instaladas y sus permisos**	**Verificar si alguna de las aplicaciones instaladas está accediendo por permisos a recursos del sistema**	
	5	**comparar estado inicial del sistema con el actual cada x tiempo**	**Hacer una verificación constante del esa del sistema**	
	6	**Entregar recomendaciones al usuario con controles sobre lo sucedido en el sistema**	**Una vez detectada y clasificada una posible anomalía entregar al usuario recomendaciones de posibles controles a ser aplicados en Android**	

GLOSARIO

Malware: es un término general para cualquier tipo de software con intenciones maliciosas. La mayoría de las amenazas online.

APK: Tipo de aplicación ejecutable para móviles Android

IOC: Indicadores de Compromiso en seguridad Informática

Controles: es el método utilizado para controlar un suceso o aplicación maliciosa

Android: Sistema operativo usado por dispositivos móviles y tabletas

XML: Formato de texto usado para trasferencia y construcción de comunicación estándar para aplicaciones y dispositivos

ANEXOS

No contemplados

DESCRIPCIÓN DE LOS GRUPOS USUARIOS DEL SISTEMA

usuario del teléfono, administrador Root

REQUISITOS NO FUNCIONALES (NFR)

La herramienta semiautomatizada, precargado en un archivo XML con la información de los IOC, adicional podrá ser instalada en dispositivos Android V 8 y 9, la herramienta no solucionara problemas de seguridad solo informara de un malware en ejecución, no alterara sin permiso alguno procesos del sistema, requerirá permisos elevados para poder ejercer algunas funciones,

será mono usuario, y actuara solo en el dispositivo no enviara información de ninguna clase afuera de Android, almacenara los registros del esta del sistema.
REQUISITOS ESPECIFICOS DE INFORMACIÓN
Acceso a información del sistema Android en cuanto en CPU Memoria y permisos.
REQUISITOS EXCLUIDOS
Interferir de forma automática en eventos presentados del sistema, o mitigar los riesgos de seguridad.
REQUISITOS DE RESTRICCIÓN
El texto presentado no puede ocupar más de una línea

1	Rendimiento del sistema
2	Escribir en los archivos Manifest del Android
3	Intervenir en el sistema
4	solicitar al usuario permisos para tomar acciones sobre el sistema

Tabla 17. Elicitación de requisitos para la herramienta semiautomatizada (construcción propia).

2.3.2 Posibles controles basado en la herramienta Semiautomatizada para Android en las versiones 8 y 9.

Los posibles controles que se expondrán a continuación hacen parte de las recomendaciones dadas desde la herramienta semiautomatizada ante una posible infección de malware.

Los controles propuestos al usuario son:

- negar los permisos a la Aplicación comprometida para:
- Escribir en Memoria
- Guardar en almacenamiento a la aplicación
- Cambiar permisos en archivos o aplicaciones
- Accesos no autorizados
- Envíos sin permiso de SMS
- Tomar sin autorización la libreta de direcciones
- Ejecutarse en segundo plano

En la siguiente tabla 18. Se toman los controles propuestos y que comportamientos se mitigaran con estos:

CONTROLES APLICABLES AL MALWARE	COMPORTAMIENTOS MALWARE
Negar Escribir en Memoria del dispositivo	Uso de memoria Ram para ejecución en segundo plano
Negar Guardar en almacenamiento a la aplicación	Acceder al almacenamiento del dispositivo
Negar Cambiar permisos en archivos o aplicaciones	Obtener la lista de aplicaciones en ejecución Obtener el registro de llamadas telefónicas, hacer y redirigir el teléfono llamadas Abrir un navegador y navegar a sitios web específicos Acceder a la cámara Grabación de un video de la pantalla

Negar Accesos no autorizados a registros del sistema	Obtención de información del dispositivo Descarga y ejecución de aplicaciones adicionales Bloquear y desbloquear de forma remota el dispositivo mediante el establecimiento de una contraseña de pantalla de bloqueo de la elección de los atacantes
Negar Envíos sin permiso de SMS, información, Contactos	Control remoto, usando varios métodos de comunicación con el servidor C&C Recolectar las credenciales ingresadas en los formularios de phishing y enviarlas al servidor C&C encriptadas no encriptadas Interceptar, redirigir, enviar y eliminar mensajes SMS, para evitar la autenticación de dos factores basada en SMS Dependiendo de los permisos obtenidos durante y después de la instalación Ejecución como proxy para enrutar el tráfico de red a través del dispositivo móvil comprometido para engañar a los mecanismos de detección de fraude de los bancos
Negar el uso sin autorización la libreta de direcciones	Obtener y editar la lista de contactos
Negar Ejecutarse en segundo plano y sobreponerse en las aplicaciones	Superposición de aplicaciones legítimas y específicas con pantallas de phishing, usando varios técnicos

	Comenzar en el inicio del dispositivo Mostrar actividad en pantalla completa para cubrir la actividad maliciosa en ejecución en segundo plano

Tabla 18 Controles y comportamientos asociados al Malware que pueden evitarse aplicándolos (Construcción propia)

Mostrar notificaciones falsas para indicar a las víctimas que inicien las aplicaciones bancarias específicas

2.3.3 Aparte del código fuente utilizado para la herramienta semiautomatizada usada en Android versiones 8 y 9

Para esta actividad, se hizo un desarrollo de una herramienta Semiautomatizada para cargar los IOC para Android y usando estos poder detectar, clasificar y ofrecer controles al usuario. El proceso de semiautomatización hace referencia a 2 circunstancias:

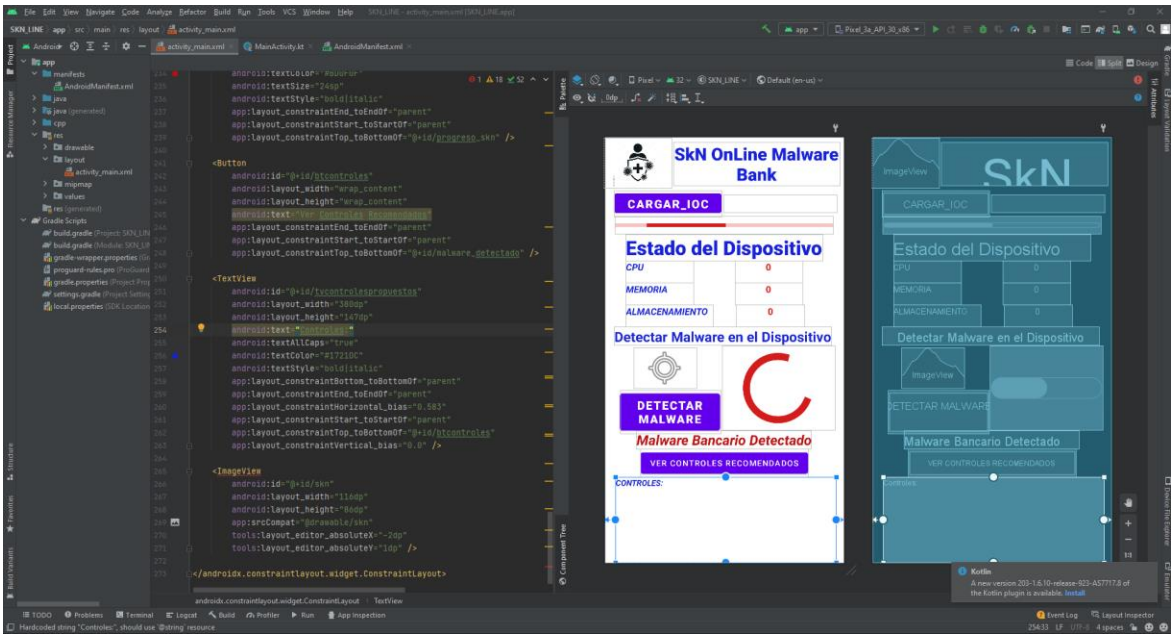
a. Que la herramienta software, aparte de hacer uso de los IoC construidos, se podría de manera manual, establecer un procedimiento para la validación con herramientas en línea como VirusTotal u otra disponible y en ese sentido, en trabajos futuros se pueden crear otras funciones que permitan su potencialización (manual o automática).
b. Los controles generados como propuesta, deben ser aplicados por el usuario final de acuerdo a las mismas necesidades.

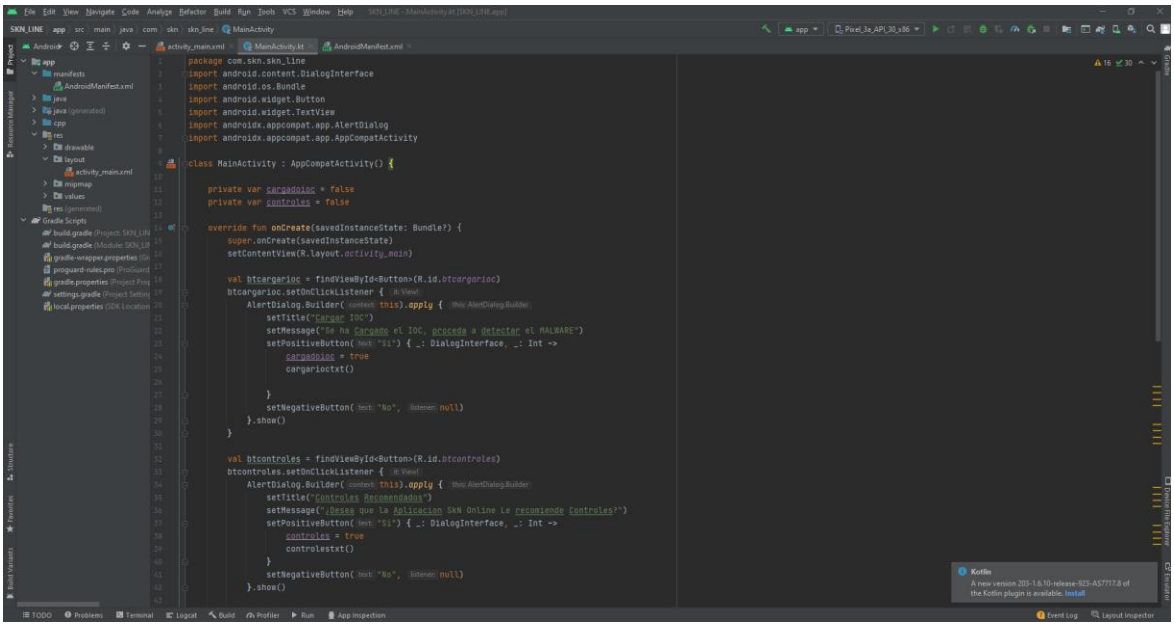
Para dicho desarrollo, se usó el Framework MIT APP Inventor [55], y Android Studio de Google, el cual permite desarrollar de una manera ágil y sencilla APKs para Android, este permite generar el diseño requerido así mismo, que permite gestionar bases de datos y aplicaciones vía web para poder realizar el control y manejo de la aplicación a si como generar las mejoras de versiones requeridas. Así mismo, tienen la capacidad de controlar el uso de memoria, la depuración del código es más sencilla, así mismo el tiempo para el

desarrollo es menor ya que cuenta con uso de líneas de código depuradas que facilitan la comprensión del desarrollador y poder tener una herramienta más eficiente.

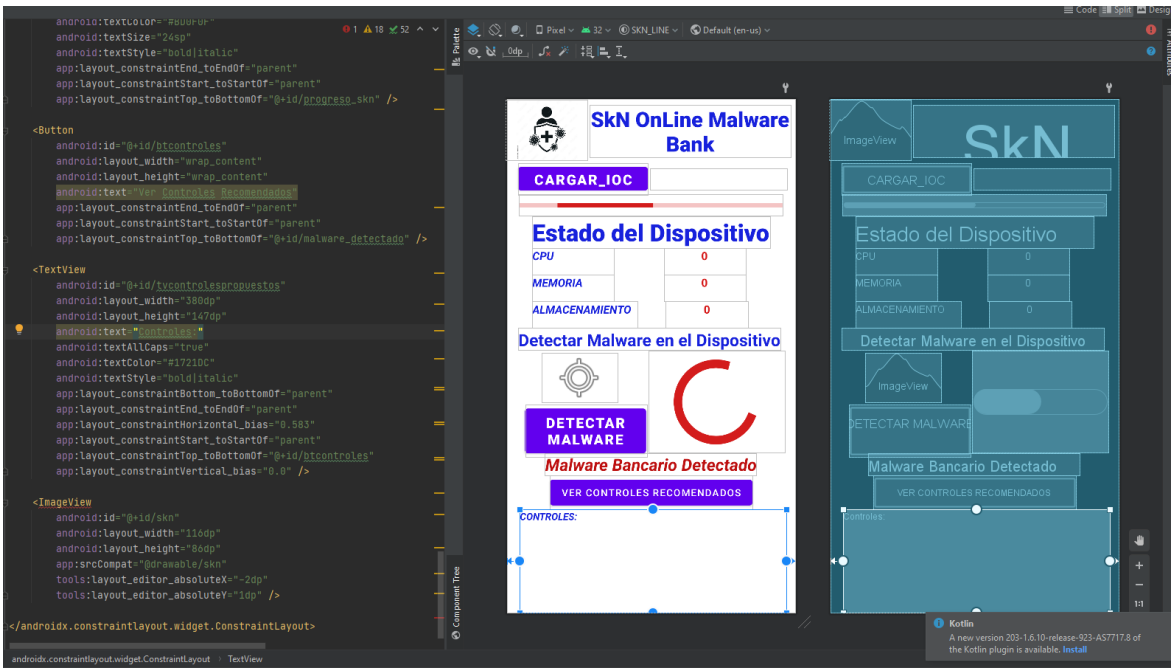
El desarrollo de la herramienta semiautomatizada, se realizó para dispositivos móviles Android bajo metodologías agiles que permiten ir teniendo resultados por partes mientras se desarrolla de manera completa el código, a continuación, se destaca aparte del código utilizado (figura 6, 7 y 8).

Figura 6. Imagen de la herramienta usada para el diseño y el desarrollo de la apk, Android Estudio Version Artic Fox. Fuente propia





En la figura 7. Apartes del código utilizado para el desarrollo de la herramienta. Fuente propia



En la figura 8. Generación de la apk de la herramienta Semiautomatizada la cual lleva por nombre SkN OnLine.

En esta fase se cumplió el objetivo de la construcción de la APK de la herramienta semiautomatizada, la cual contiene la lógica para la detección y clasificación del malware con el que se trabajó esta tesis el cual es CERBERUS.

2.4 Fase 4: Verificar el proceso de detección, clasificación, y contención rápida a través de la ejecución de la aplicación en Android

Para verificar el proceso fue necesario la construcción de un ambiente controlado para desarrollo de las pruebas por lo cual se utilizó para el desarrollo del mismo, el emulador NOXPlayer V 7.019 el cual es gratuito y permite emular terminales móviles en las versiones requeridas o desde la 7.0 de Android y para nuestro caso la Versión 8 y 9.

En ese sentido, se desarrollaron las siguientes 3 actividades:

- Diseño del ambiente controlado y las pruebas a realizar.
- Evaluar la Herramienta Semiautomatizada por medio de pruebas al Dispositivo Controladas
- Validar los controles generados como recomendación

2.4.1 Actividad 1: Diseño del ambiente controlado y las pruebas a realizar.

Para el diseño del ambiente controlado para la realización de las pruebas, se contó con, el uso de un emulador para dos dispositivos móviles Android Pie: 9.0 y Android 8.0 Oreo.

Las pruebas realizadas se definieron mediante una matriz de amenazas comunes recolectadas en los IOC, y los que más afectan las versiones de Android 8 y 9 y finalmente se tomó para las pruebas en el ambiente controlado el **CERBERUS** Cepa que se descargó de unos de los repositorios antes descritos para Malware Bancario, para la verificación de la detección, posterior clasificación y recomendación al usuario infectado, todo esto mediante la precarga de la aplicación con el IOC correspondiente a CERBERUS.

Resultados obtenidos en la Actividad 1 de la fase 4:

Inicialmente se creó en el emulador las dos versiones usadas en este laboratorio (en el emulador NOXPlayer como se observa en la figura 9)

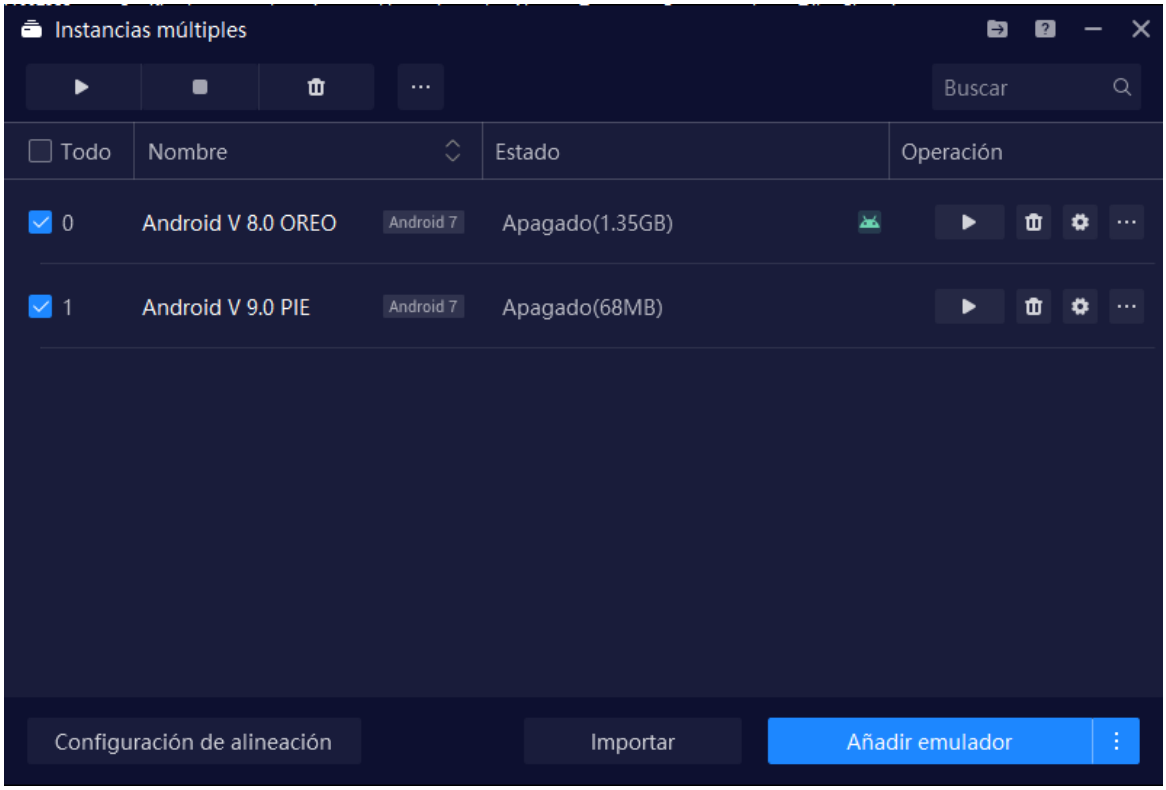


Figura 9. Emulador de dispositivos Móviles con las versiones usadas en el laboratorio 8 y 9 y soportando desde la versión 7 de Android el desarrollo de las pruebas así se pudo abarcar muchos más dispositivos. Fuente propia.

Así mismo se encendieron los emuladores para cargar la aplicación APK semiautomatizada desarrollada para la tesis.

Luego de tener el Emulador funcionando se procedió a detallar el proceso de carga de la apk, el análisis de las pruebas y el flujograma de las mismas para obtener resultados, para ello, se construyó un procedimiento que fue usado en el desarrollo del laboratorio. Por otro lado, se cargó la herramienta para ser instalada y ejecutada en las versiones Android

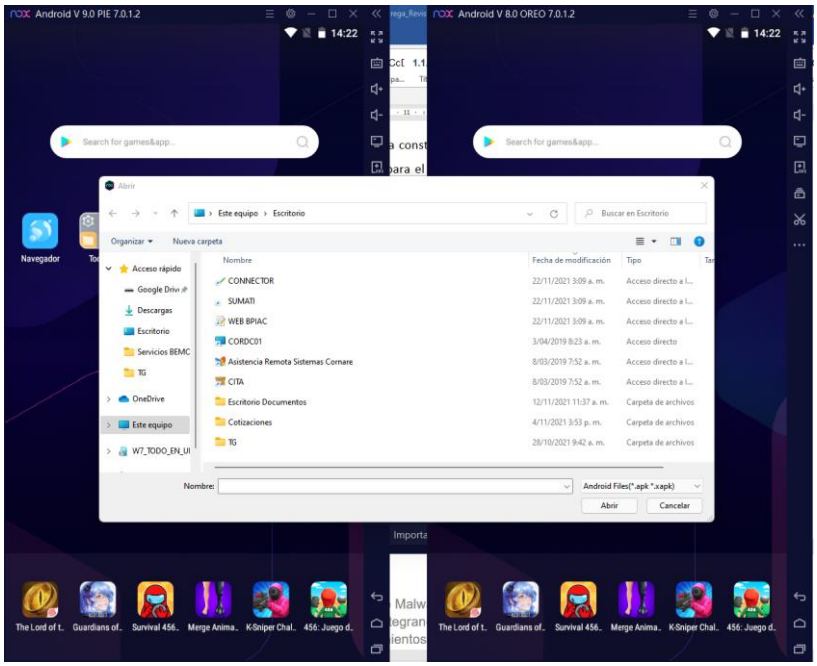


Figura 10. Instalación de la Aplicación Semiautomatizada en el emulador Android, como se observa la imagen se carga el archivo APK.

Se puede observar en las figuras 11, 12, 13, 14 y 15 el paso a paso de la carga de la Aplicación APK semiautomatizada.

Figura 11. Carga de la aplicación en archivo APK en el emulador, para poder ser instalada y ejecutada.

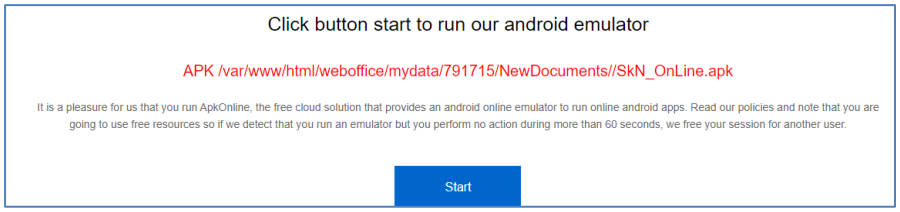


Figura 12, Inicializando emulador para la Carga de la APK, el emulador es el ambiente controlado para evitar que el Malware afecte dispositivos usados normalmente.

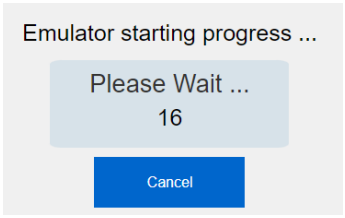


Figura 13. una vez Lista la carga de la APK en el Emulador, podemos proceder a abrir la aplicación instalada.

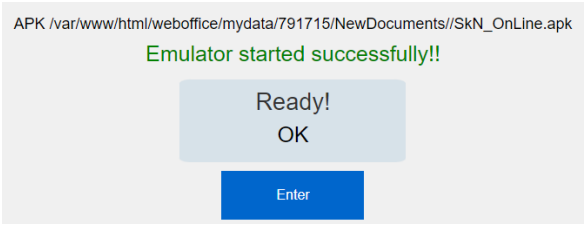
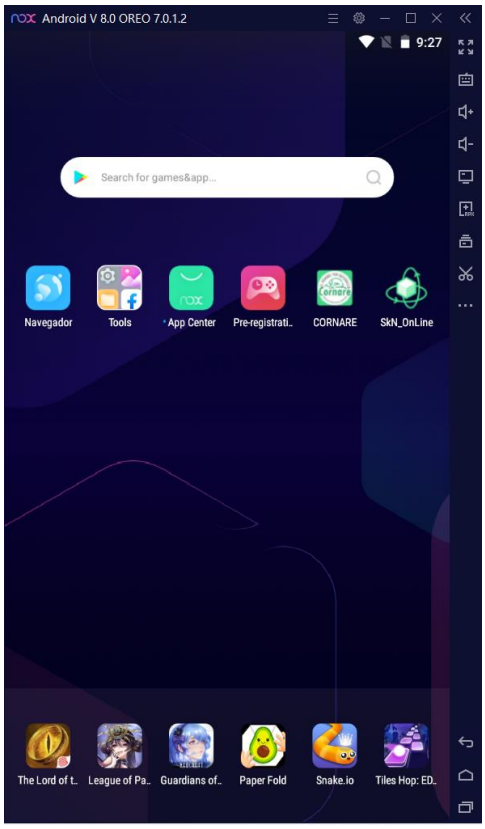


Figura 14. En esta figura se observa la APK Instalada, en el escritorio de emulador para poder ser ejecutada.



A continuación, se realiza la ejecución de la Aplicación Semiautomatizada y se pasa a explicar el funcionamiento, así como los menús de la misma como se observa en la figura 15.

Figura 15. Menús Apk de la herramienta semiautomatizada Instalada, en la cual se observan el nombre de la aplicación, botón de carga de los IOC y botón de búsqueda del Malware. Fuente propia

Dentro de la aplicación podemos observar en la figura 15 que se construyó de manera muy básica enfocando la misma en su ejecución y cumplimiento del objetivo general el cual es Leer el IOC en este caso CERBERUS, para luego poder detectarlos según las características descritas en el archivo IOC

En la figura 15 se muestra en la parte superior el nombre de la aplicación, SKN ONLINE MALWARE BANK más abajo un botón con el que lee el IOC que para nuestro caso es el XML de CERBERUS el Malware bancario con el que se trabajó este laboratorio controlado. Como se observa en la figura 15, una vez cargado y el dispositivo infectado se procede a realizar el escaneo del Móvil.

En la figura 16 siguiente podemos observar la carga de los IOC

Figura 16. En esta figura se carga los IOC previamente en el teléfono.

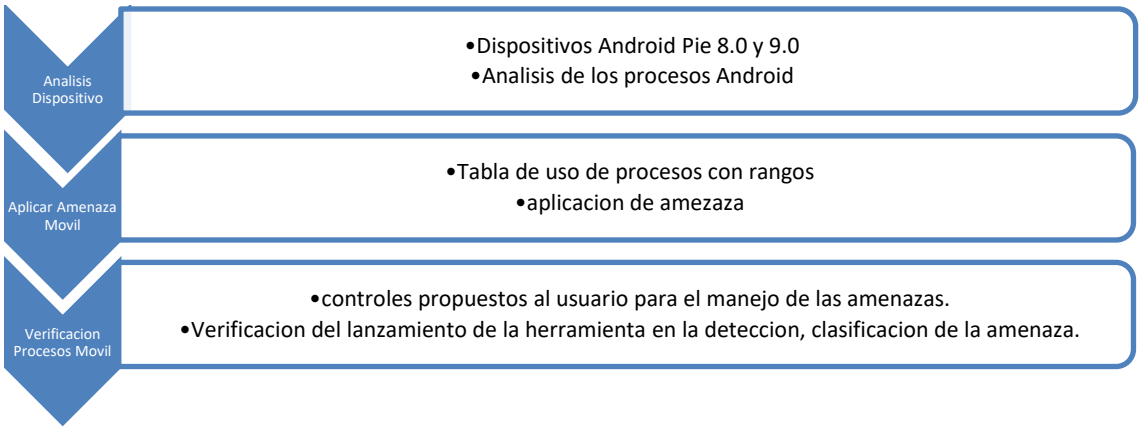
Las pruebas que se realizaron para este ambiente controlado se basaron en la carga del Indicador de Compromiso en nuestro caso Malware CERBERUS, con él cual se procedió a realizar la infección del dispositivo mediante él envió de un archivo vía mensaje de texto con una URL para descarga o el WhatsApp, o través de una APK de descarga.

Para lo anterior y el cumplimiento de las pruebas este será el paso a paso para la ejecución de la aplicación semiautomatizada para la detección, clasificación y entregar posibles controles al usuario:

1. Lectura el IOC precargado en la herramienta semiautomatizada

2. Descargar de un repositorio de Malware la Cepa que en este caso para trabajar en el ambiente controlado será CERBERUS: Hash 84da367dd962210f27858799fe25d79f.
3. Compilar el Malware y ponerlo en un archivo ejecutable.
4. Enviar el Malware Vía correo electrónico, Mensaje de texto, o WhatsApp o través de una APK de descarga.
5. Comprometer el dispositivo abriendo y ejecutando la URL y el archivo con la infección en el ambiente controlado.
6. Ejecutar el Escaneo con la aplicación SkN_OnLine en el dispositivo comprometido y por medio de la revisión de los IOC identificar y clasificar la amenaza objeto de este laboratorio controlado.
7. Entregar al usuario mediante mensaje Recomendaciones para su contención

Con lo anterior se da por cumplida la actividad de esta fase la cual comprendía la ejecución de un ambiente de pruebas controlado en este caso con NOX y las pruebas que se realizaron en este ambiente. En consecuencia, el análisis realizado fue el siguiente:
Figura 17. Proceso de análisis y aplicación de amenaza en un dispositivo móvil, en la figura se observa la carga del virus el cual es una apk adicional se confirma que corresponda el hash en imágenes posteriores. Construcción Propia



Con esto, se ha configurado el respectivo ambiente controlado para las pruebas.

2.4.2 Actividad 2: Evaluar la Herramienta Semiautomatizada por medio de pruebas al Dispositivo Controladas.

La evaluación se hizo mediante la toma de muestras de los diferentes procesos Android afectados por el Malware CERBERUS descrito previamente en los IOC, para así poder verificar el cumplimiento del objetivo de la herramienta semiautomatizada, para lograr la evaluación correcta de la herramienta, se estableció un protocolo para la validación de acciones previas y el estado después de la aplicación de las pruebas (figura 18).

Para el desarrollo de pruebas se carga el ambiente controlado, que para caso es el emulador NOX con la aplicación previamente cargada (figura 18).

Resultados obtenidos en la Actividad 2 de la fase 4:

Figura 18. Emulador con la aplicación instalada con la cual se realizarán las pruebas. Fuente propia.

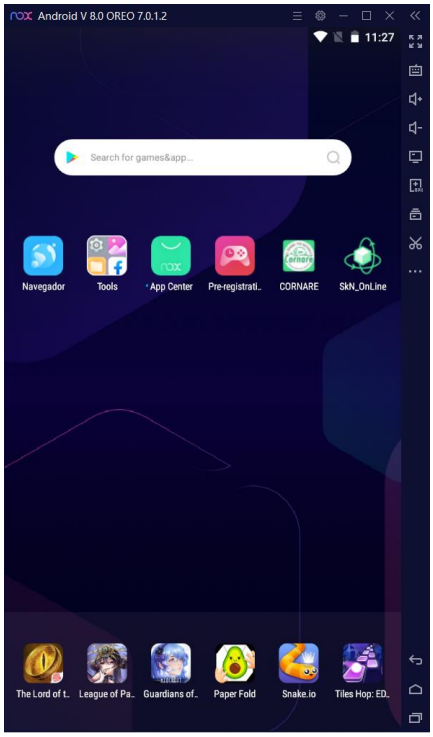
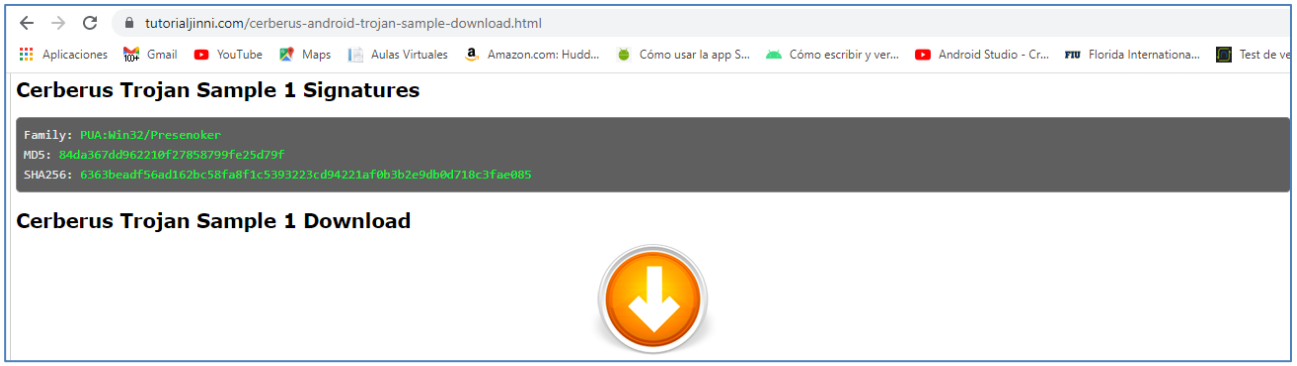


Figura 19. En la siguiente figura podemos observar el resultado de abrir la aplicación semiautomatizada, la cual nos ofrece varios menús, para la carga del IOC y el escaneo al dispositivo:

Figura 20. En la figura siguiente se abre el menú de Leer IOC y se realiza la precarga del archivo XML, con la información del malware Bancario para realizar el escaneo en el dispositivo la precarga de los IOC con el XML de CERBERUS como se observa en la figura.

Una vez cargado el IOC, se procede con la descarga del repositorio del Malware CERBERUS para realizar la prueba en el ambiente controlado como se observa en la figura 21.

Figura 21. En la siguiente figura realizamos el ingreso y búsqueda del Malware con el que se realizó el laboratorio controlado para nuestro caso Cerberos Trojan Ingreso al repositorio de MALWARE:



Se verifica el Hash corresponde al descrito en los IOC: 84da367dd962210f27858799fe25d79f en la página de virus total para estar seguros de que el Malware Bancario sea el correcto para este laboratorio, como se observa en la figura 22 y 23.

Figura 22. Búsqueda del Hash del Malware Bancario en la plataforma virus total.

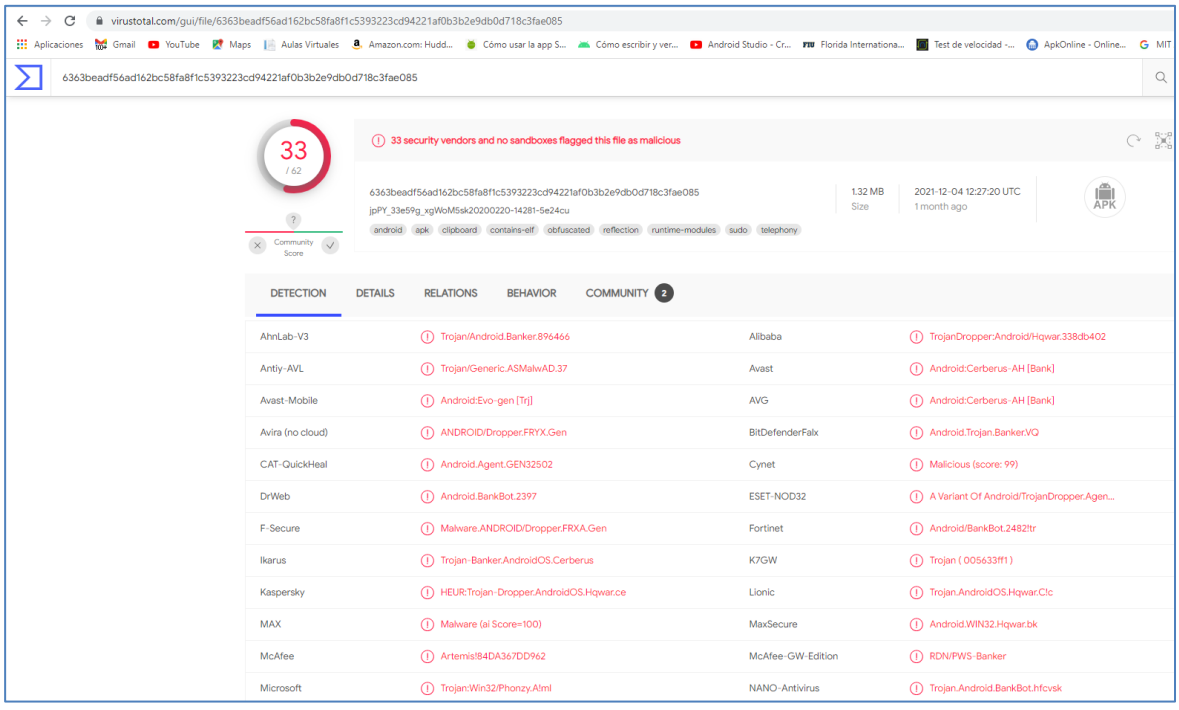
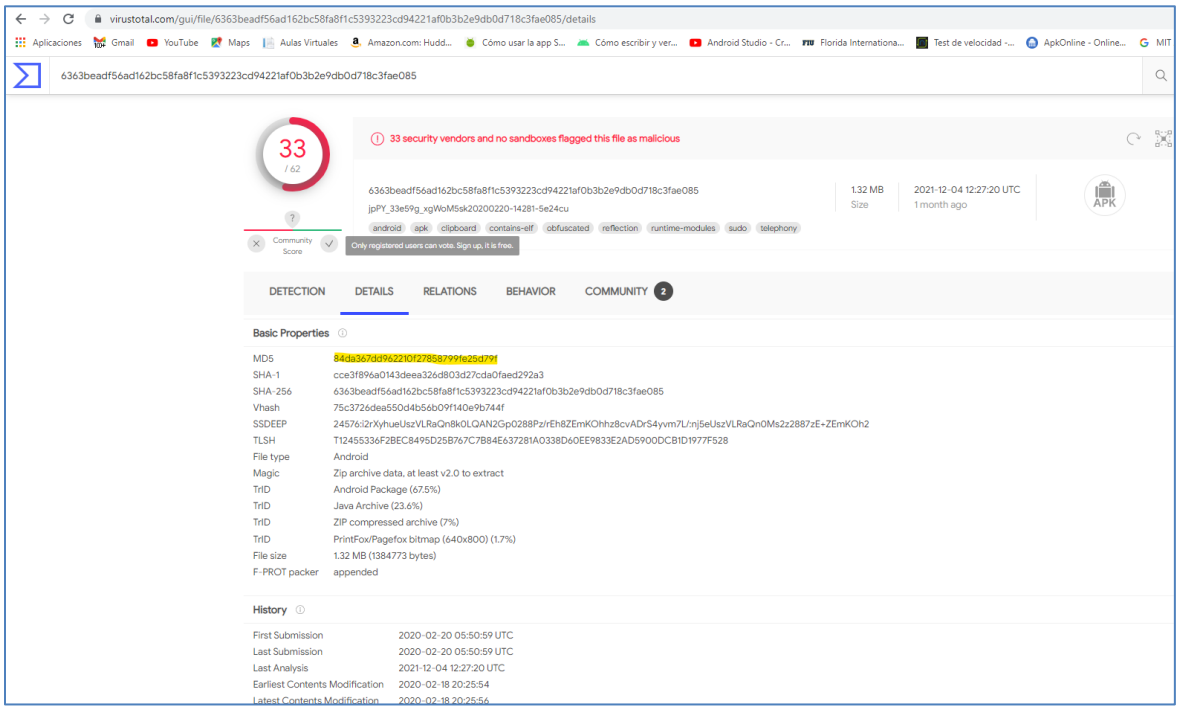


Figura 23. En la siguiente figura se compara el hash del malware Cerberus, con el arrojado por virus total, del apk descargado para asegurarnos que coincide:



Seguidamente, se realiza la descarga del Malware Bancario CERBERUS para su preparación y envío para infección, que, para la prueba, es la aplicación Móvil con la APK que usualmente con engaños en este caso con la pandemia y el coronavirus es una aplicación con este tema:

Figura 24. En la siguiente figura se observó y se realizó la descarga del Malware Bancario CERBERUS

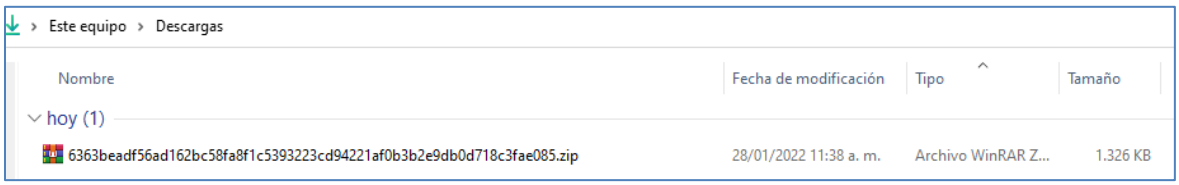


Figura 25. En la figura siguiente se verifica la APK descargada la cual contiene el Malware Bancario CERBERUS el cual fue descargado del repositorio de Malware y el cual se usó para este laboratorio controlado en Android.

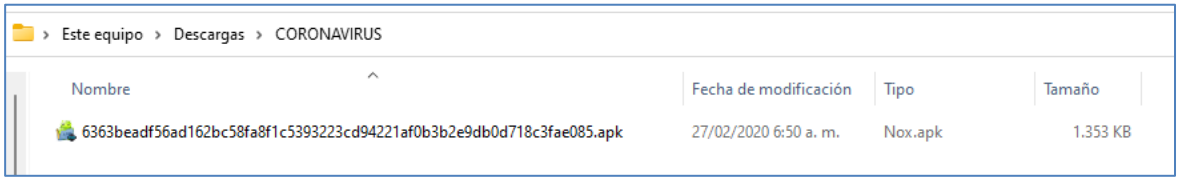


figura 26. En la siguiente figura se busca la aplicación descargada en el equipo de cómputo y se carga la APK en el Emulador Android, para realizar la infección por medio de la instalación como se muestra en la figura.

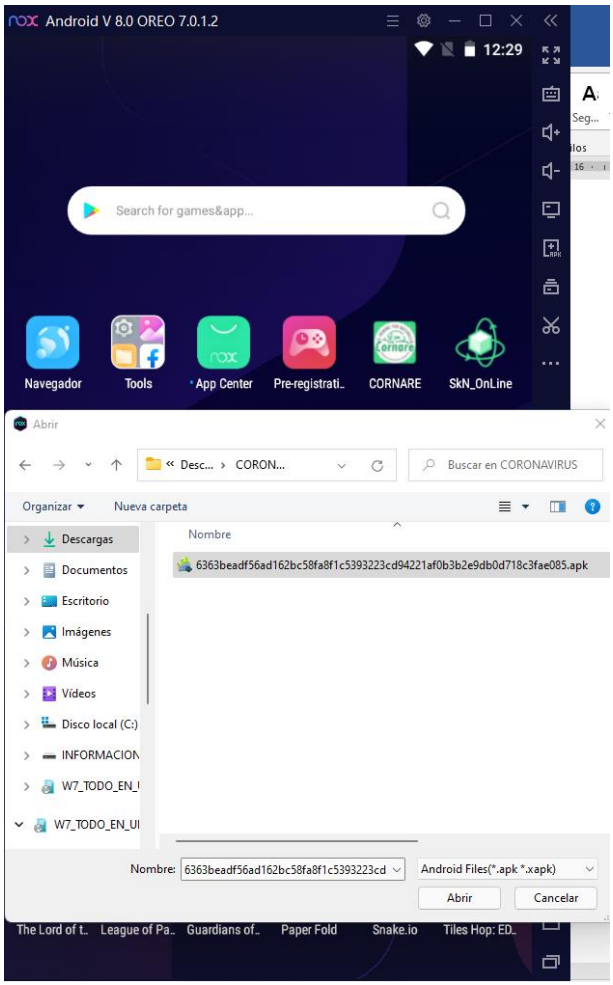


Figura 27. En la siguiente imagen una vez cargada la apk maliciosa, esta se instala y figura con el nombre de flash player, la cual se ve inofensiva a los usuarios como se observa en la Figura

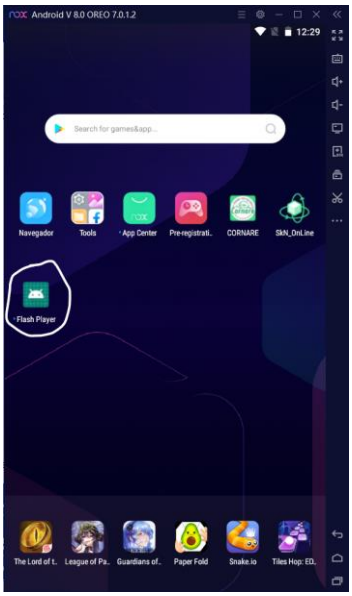
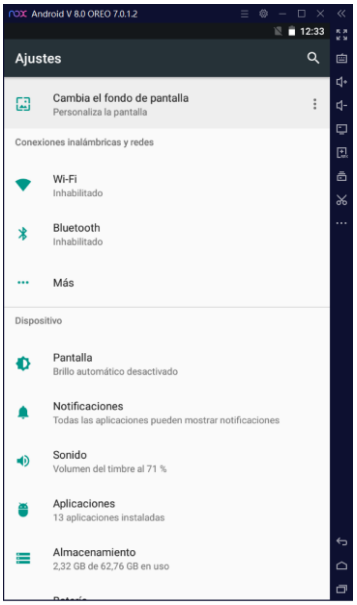
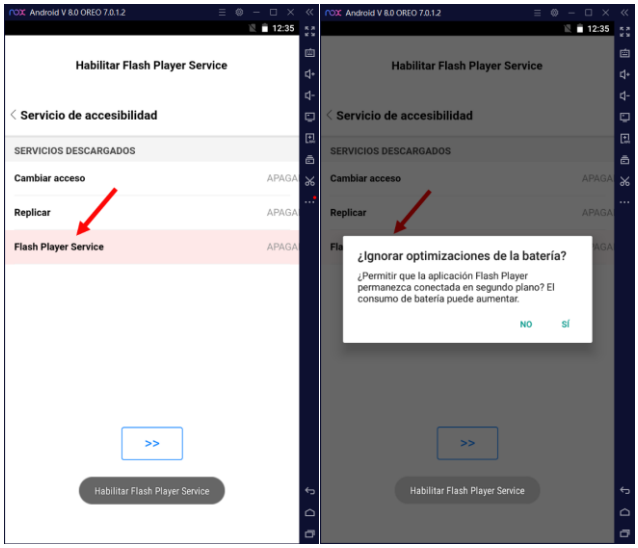


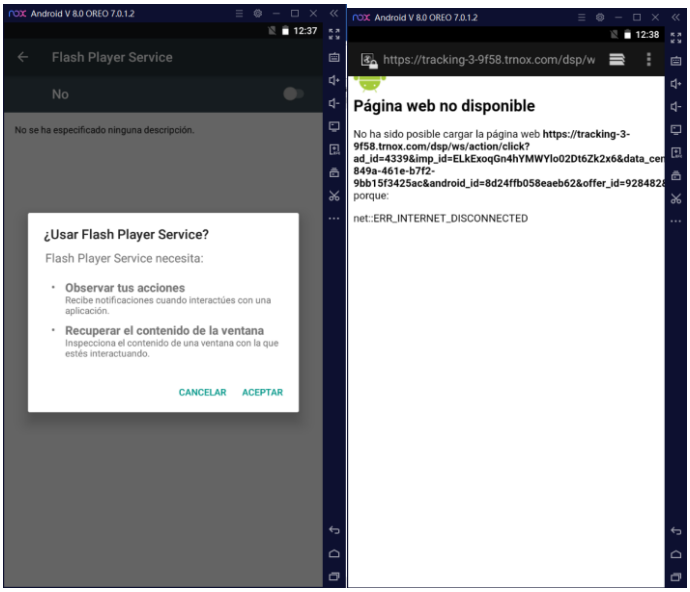
Figura 28. En la siguiente imagen se realizó la ejecución de la aplicación maliciosa en el Emulador, con la cual se logra infectar el dispositivo con el candidato Malware Cerberus:



Con la anterior imagen 28 se logra ejecutar para Propagar la infección en el dispositivo para posteriormente escanear con la herramienta semiautomatizada igualmente se deshabilita el WIFI para evitar propagación del Malware a otros dispositivos como se observa en la figura.

Figura 29. En la siguiente imagen, procedemos a ejecutar la aplicación e infectar el dispositivo, la cual exige al usuario dar permisos sobre algunos parámetros del sistema entre ellos el envió de notificación lectura del disco, aplicaciones y contactos como se observa en la figura.





En las imágenes anteriores figura 29 se puede observar como el dispositivo es comprometido pidiendo una serie de permisos y habilitando diferentes componentes que requiere para conectarse al servidor de Comando y Control y finalmente trata de comunicarse para terminar de bajar la infección, sin embargo, dado que el equipo está aislado de la red (pruebas controladas) , dichas peticiones son fallidas, pero el dispositivo se encuentra ya comprometido.

Ahora se procede a ejecutar la herramienta semiautomatizada a la que previamente se cargó el IOC para detectar y clasificar el MALWARE bancario CERBERUS (figura 30).

Figura 30. En la siguiente imagen veremos la detección y clasificación de la amenaza en el teléfono, mediante el uso del IOC previamente cargado y ejecutando el escaneo específico del indicador para Cerberus Malware Bancario. Fuente propia.

Como se observa en la figura anterior la herramienta semiautomatizada detecta el Malware en tiempo real, e informa de los componentes comprometidos según el contenido del IOC cargado, que para el caso tenemos:

android.permission.READ_PHONE_STATE

android.permission.SEND_SMS

android.permission.RECEIVE_SMS

android.permission.CALL_PHONE

android.permission.RECORD_AUDIO

android.permission.INTERNET

android.permission.WRITE_EXTERNAL_STORAGE

android.permission.READ_CONTACTS

android.permission.READ_SMS

android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

android.permission.REQUEST_DELETE_PACKAGES

android.permission.READ_EXTERNAL_STORAGE

android.permission.RECEIVE_BOOT_COMPLETED

android.permission.USE_FULL_SCREEN_INTENT

android.permission.ACCESS_NETWORK_STATE

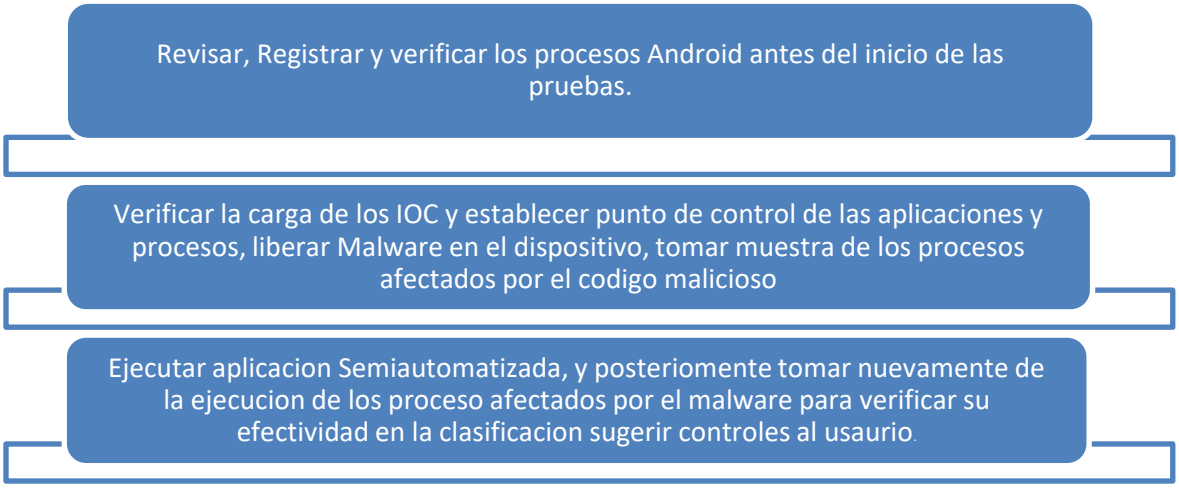
android.permission.WAKE_LOCK

android.permission.FOREGROUND_SERVICE

android.permission.GET_ACCOUNTS

Por lo anterior, se puede observar que fue detectado el Malware e identificado por su modus operandi que previamente se precargo en los IOC logrando identificar y clasificar los componentes comprometidos como se observa en la imagen anterior, en donde se observan 12 componentes comprometidos y descubierto por la herramienta.
En la siguiente imagen veremos un paso a paso de la forma como actúa la herramienta hasta lograr informar al usuario de los posibles controles a aplicar por el en el dispositivo (figura 31).

Figura 31. Controles y verificación de la herramienta automatizada paso a paso como identifica el objetico en este caso el Malware Bancario Cerberus. Construcción propia



Con lo anterior en la figura 31 se da cumplimiento al Objetivo y actividades planteadas en el desarrollo de esta fase con la carga de los IOC, Búsqueda de coincidencias que contiene el XML con el cual se compara e identifica la afectación y el proceso en el teléfono.

2.4.3 Actividad 3: Validar los controles generados como recomendación

Mediante el uso medido de los procesos Android, en contraste con los procesos ya descritos que tuvieron la afectación los cuales se encuentran en los IOC, se toman los procesos que afectarían el Malware, en un estado normal, y posterior a eso se verifican cada uno de los procesos afectados, y finalmente después de la mitigación con la herramienta semiautomatizada se verifica nuevamente estos procesos, se comparan la primera muestra y la última y estas deben ser iguales, con los cual se tendría un método de comparación de procesos (antes y después).
Resultados obtenidos en la Actividad 3 de la fase 4:

En la imagen de la Figura 32 podemos observar que se ofrecen controles y sugerencias para ser aplicadas por el usuario desde el dispositivo.

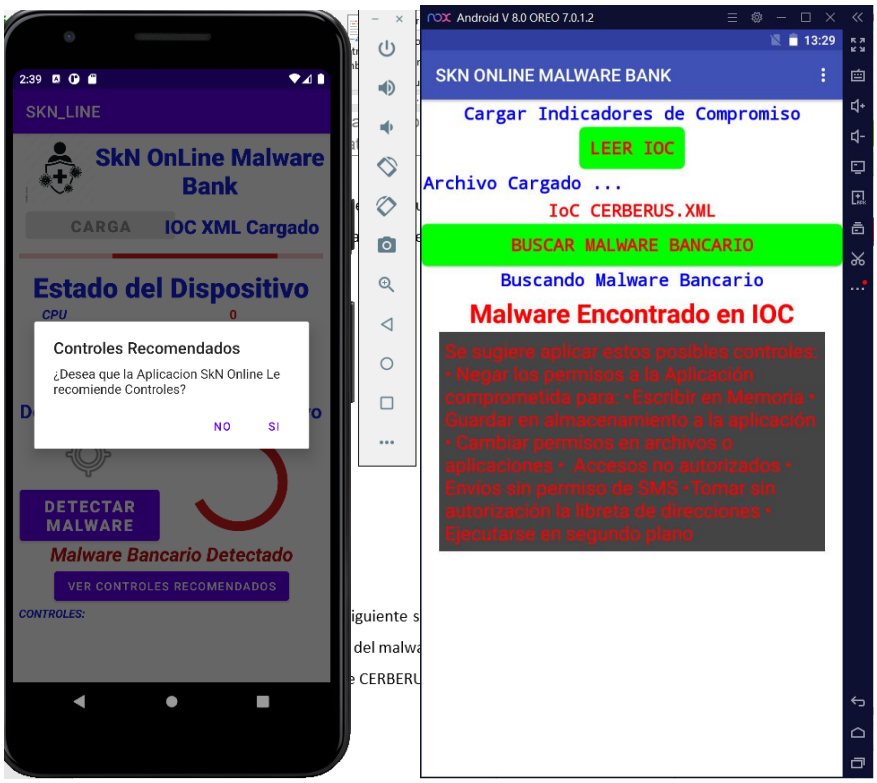


Figura 32. En esta imagen la herramienta semiautomatizada entrega posibles controles para aplicar manualmente por parte del usuario.

Controles sugeridos por la herramienta semiautomatizada:

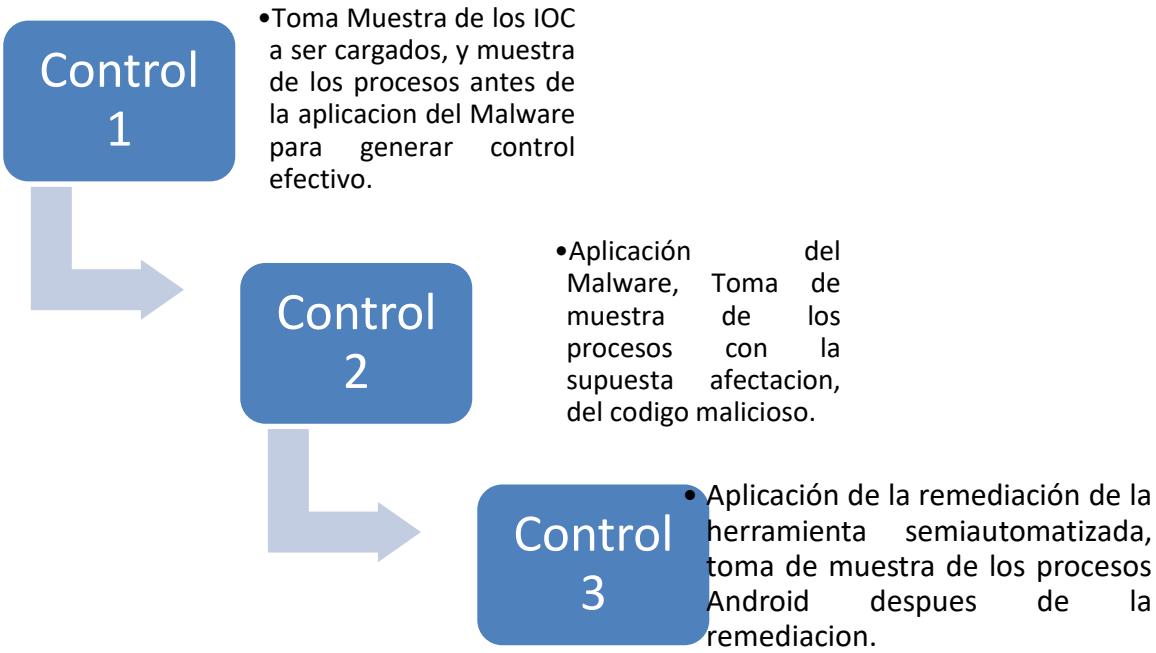
- Negar los permisos a la Aplicación comprometida para:
- Escribir en Memoria
- Guardar en almacenamiento a la aplicación
- Cambiar permisos en archivos o aplicaciones
- Accesos no autorizados
- Envíos sin permiso de SMS
- Tomar sin autorización la libreta de direcciones
- Ejecutarse en segundo plano

Controles Aplicados a la actividad 3

En la siguiente figura se propuso algunos controles para ser aplicados en los dispositivos por parte de los usuarios y así mitigar la ejecución y daño causado por el malware.

Estos serían algunos controles sugeridos (figura 3):

Figura 33. Controles Aplicables a la actividad 3



Con las fases anteriores y el cumplimiento de las mismas en cada actividad, se puede dar por cumplido el objetivo general el cual tiene como elemento principal la detección y clasificación de los MALWARE Bancarios, así como generar una herramienta Semiautomatizada, la cual por no ser intrusiva depende de las acciones del usuario para poder ejecutarse, adicional a esto, se entrega o da a conocer algunos controles aplicables al dispositivo por parte del usuario y no automáticamente para no ser intrusivos y las decisiones provengan del propietario del dispositivo.

3. Conclusiones y recomendaciones

3.1 Conclusiones

- El resultado obtenido en este trabajo de grado, se basa en el comportamiento de un software malicioso, el cual va dirigido a dispositivos móviles Android en sus versiones para nuestro caso 8 y 9, al estudiar cada uno y su forma de infección, propagarse, procesos que afecta, así como los procesos requeridos dentro del móvil, nos da una pista para poder detener o identificar de manera acertada el Malware Bancario.
- Todo el Malware estudiado en esta tesis dirigido al tipo bancario, nos da pistas de el comportamiento similar o igual de este tipo de código malicioso, ya que su modus operando es el mismo en todos los casos, empezando por la infección, la manera como llega el malware Bancario al dispositivo, los permisos que solicita el Malware al Android los cuales siempre sin similares, procesos de lectura de almacenamiento, galería, contactos del teléfono entre otros.
- Se logro identificar de manera rápida cada aplicación maliciosa, debido a que todas las aplicaciones .APK para Android contienen un archivo Android.manifest el cual al descomprimirse para ser instalado en el móvil, contiene todos los procesos requeridos para cada aplicación que de manera acertada en el caso del malware bancario siempre son los mismos, logrando identificar y clasificar inmediatamente Malware de tipo bancario.
- Con los resultados obtenidos a partir de la investigación, selección, construcción y pruebas de seguridad en dispositivos de tipo Smartphone, se puede fortalecer la seguridad en dichos dispositivos móviles, permitiendo a los usuarios finales tomar acciones para reducir las brechas de seguridad.
- Con respecto al objetivo 1 que se trato de “Caracterizar los diferentes Indicadores de Compromiso que puedan ser usados o desarrollados en Android en sus últimas 2 versiones más usadas, con el fin de detectar posibles ataques informáticos tipo Malware” se logró de manera exitosa, logrando caracterizar cada uno de los

indicadores de compromiso, encontrar y usar las versiones de Android con más uso en dispositivos Smartphone (para el año 2020), así mismo, con los IOC identificados y construidos se hizo más fácil la identificación de amenazas y su afectación para poder desarrollar los demás objetivos.

- Adicional a lo anterior se identifico de manera exitosa la manera de clasificar y detectar rápidamente el malware bancario, mediante el archivo empaquetado en la APK maliciosa llamado Manifest.xml
- En el objetivo 2 que se trataba de “Proponer un mecanismo de clasificación de acuerdo al nivel de impacto de las amenazas informáticas”, Se logró desarrollar de manera exitosa, con lo cual se propuso un mecanismo de clasificación de acuerdo al nivel de impacto de las amenazas, con esta clasificación se logró identificar cual amenaza afecta potencialmente mayor el dispositivo que afecta y donde lo afecta.
- En el objetivo 3 que se trataba de “Diseñar una aplicación que permita la incorporación de Indicadores de Compromisos para la detección de manera semiautomática los diferentes ataques, generando posibles controles.”, se logró certeramente diseñar una aplicación funcional que de manera acertada puede los IOC con la información necesaria para poder identificar las amenazas tipo malware bancario, y con esta información identificarla adecuadamente como malware bancario mediante los IOC cargados pudiendo clasificarla adecuadamente con el IOC .
- En el objetivo 4 que se trataba de “Verificar la pertinencia en el proceso de detección clasificación, y contención rápida a través de la ejecución de la aplicación en Android.”, se logra la conjugación de toda la tesis dado que es el resultado final de la ejecución acertada de la herramienta semiautomatizada logrando la detección clasificación y proponiendo posibles controles a los usuarios de los dispositivos. Final mente el objetivo general se da por cumplido donde se trata de “Identificar las amenazas informáticas de tipo Malware bancario o Ransomware Móvil hacia dispositivos Android, con el uso los IOC a través de una herramienta semiautomatizada con el fin de detectar, clasificar y sugerir una propuesta de controles”, dado que se logró la identificación clasificación y generación de posibles controles, los cuales con la herramienta semiautomatizada el usuario puede tomar decisiones en cuanto aplicarlas o no.

Como recomendaciones generales fue un acierto la construcción de la herramienta semiautomatizada dado que a pesar que en el mercado hay muchas herramientas antivirus no se enfocan en los Indicadores e compromiso como posible fuente para detectar y clasificar amenazas si no que estas se basan en firmas que muchas veces pueden cambiar con cada mutación mientras que con los comportamientos si bien es cierto se generan falsos positivos se puede estar mucho más alerta de lo que pasa con el dispositivo, igualmente al ser una herramienta semiautomatizada esta necesariamente actúa con el usuario para tomar y emprender acciones, y así proteger si es el caso el teléfono.

El otro gran acierto fue identificar las aplicaciones según los permisos solicitados ya que todos se contienen en un mismo archivo, el manifest.xml.

3.2 Recomendaciones

Teniendo en cuenta que existen muchos repositorios de IOC en el mercado sugiero conectar en un futuro esta herramienta directamente a estos y así mantenerla actualizada, dado que para esta versión se construyeron manualmente lo cual es engorroso y lleva mucho tiempo realizarlo, aunque es muy eficiente la detección después de construidos los IOC sería bueno que estos se tomaran directamente y automáticamente de los repositorios.

Adicionalmente, mantener una actualización constante de la herramienta dado el cambio en códigos maliciosos o sus mutaciones para poder hacer más seguro y precisa la detección del Malware Bancario.

Adicional para una versión posterior hacer esta herramienta automática del todo y que se ejecute en segundo plano realizando periódicamente escaneos automáticos e informe de posibles infecciones pero que también estas sean remediadas automáticamente denegando permisos en aplicaciones o uso de recursos del dispositivo.

Para futuras pruebas tener un mejor ambiente de pruebas dado que al trabajar con malware se pueden presentar problemas de infección en los propios equipos y dispositivos lo cual causa problemas en la actividad desarrollada.

Como recomendación central para el mejoramiento de la herramienta se propone, realizar a parte de la detección y clasificación una mitigación inmediata y en línea en el momento que se desempaquete la aplicación, mediante la lectura del Manifest identificando los mismos permisos usados por estas aplicaciones maliciosas que son:

android.permission.READ_PHONE_STATE

android.permission.SEND_SMS

android.permission.RECEIVE_SMS

android.permission.CALL_PHONE

android.permission.RECORD_AUDIO

android.permission.INTERNET

android.permission.WRITE_EXTERNAL_STORAGE

android.permission.READ_CONTACTS

android.permission.READ_SMS

android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

android.permission.REQUEST_DELETE_PACKAGES

android.permission.READ_EXTERNAL_STORAGE

android.permission.RECEIVE_BOOT_COMPLETED

android.permission.USE_FULL_SCREEN_INTENT

android.permission.ACCESS_NETWORK_STATE

android.permission.WAKE_LOCK

android.permission.FOREGROUND_SERVICE

android.permission.GET_ACCOUNTS

Con los permisos anteriores identificados la probabilidad de que sea un malware tipo bancario es del aproximadamente el 80%, lo cual se puede complementar con conexiones a puertos poco seguros o proxy reverse, adicional a las descargas que continúan después de instalada una aplicación que no tiene razón de ser con la instalación inicial.

Bibliografía

[1] SIGITE '16: Proceedings of the 17th Annual Conference on Information Technology Education September 2016 p. 54–59 https://doi.org/10.1145/2978192.2978218

[2] ALVAREZ, Víctor YARA Documentation. {En línea}. {29 enero de 2021} disponible en: https://media.readthedocs.org/pdf/yara/latest/yara.pdf. 117 p.

[3] ANDROID DEVELOPERS. Guia de usuario, Firmar tu aplicación. {En línea}. {21 febrero de 2021} disponible en: https://developer.android.com/studio/publish/app-signing?hl=es

[4] BENZMÜLLER, r. Malware trends 2017. {En línea}. {04 octubre de 2017} disponible en: https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017. 1 p.

[5] CAMARGO, l. m. p., Galindo, J. C. A., & Vega, J. J. C. (2013). Seguridad En Dispositivos Móviles

Con Sistemas Operativos Android Y Ios. Tecnología Investigación y Academia, 1(2), 42–59. Retrieved from http://revistas.udistrital.edu.co/ojs/index.php/tia/article/view/4312 CCN, C. C. nacional. (2013). Indicadores de compromiso (IOC).

[6] Casey, E. (2011). Handbook of digital forensics and investigation. Burlington, Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard.

[7] Cohen, M. I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the ompromiso. Digital investigation, 8, S101-S110.

[8] Chen, J. (2020). Android Operating System Definition. Updated Feb 13, 2020. https://www.investopedia.com/terms/a/android-operating-system.asp.

[9] Chen, L., Hou, S., & Ye, Y. (2017). SecureDroid. Proceedings of the 33rd Annual Computer Security Applications Conference on - ACSAC 2017, 362–372. https://doi.org/10.1145/3134600.3134636

[10] Diseño de un Entorno Open Source para Análisis Automatizados de Malware. Manuel Martín Gutiérrez. Universidad de Sevilla. 2019 http://bibing.us.es/proyectos/abreproy/92267/fichero/TFG-2267-MARTIN.pdf

[11] Dong-Jie, W., Ching-Hao, M., Hahn-Ming, L., Kuo-Ping, W., & I, A. P. (2012). Droidmat: Android Malware Detection Through Manifest and Tracing. In Proceedings of the Seventh Asia Joint Conference on Information Security.

[12] Du Yao, Wang Xiaoqing, W. J. (2014). A static Android malicious code detection method based on multi-source fusion. International Journal of Applied Engineering Research, 9(22), 5968– 5974. https://doi.org/10.1002/sec

[13] Elenkov, N. (2015). Android Security Internals. Network Security (Vol. 2015). https://doi.org/10.1016/S1353-4858(15)30046-5

[14] D. V. Eduardovich and Y. A. Vladimirovich, "Reputation risks through information security incidents," 2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg, 2016, pp. 194-198, doi: 10.1109/EIConRusNW.2016.7448152.

[15] El valor de los indicadores de compromiso en la industria. INCIBE. 8 de marzo de 2018. https://www.incibe-cert.es/blog/el-valor-los-indicadores-compromiso-industria

[16] Elish, K. O., Shu, X., Yao, D., Ryder, B. G., & Jiang, X. (2015). Profiling user-trigger dependence for Android malware detection. Computers and Security, 49(540), 255–273. https://doi.org/10.1016/j.cose.2014.11.001

[17] Emm, D., Unuchek, R., Garnaeva, M., Ivanov, A., Makrushin, D., & Sinitsyn, F. (2016). IT THREAT EVOLUTION IN Q2 2016 IT threat evolution in Q2 2016. Overview. Retrieved from https://securelist.com/files/2016/08/Kaspersky_Q2_malware_report_ENG.pdf

[18] Han, H., Chen, Z., Yan, Q., Lizhi, P., & Zhang, L. (2015). A Real-time Android Malware Detection System Based on Network Traffic Analysis. Algorithms and Architectures for Parallel Processing, 9530, 504–516. https://doi.org/10.1007/978-3-319-27137-8_37

[19] Heras. C, I., & Sierra. L, D. (2015). Sistema de Deteccíon de Malware en Android.

[20] Homem, I., Kanter, T., & Rahmani, R. (2016). Improving distributed forensics and incident response in loosely controlled networked environments. International Journal of Security and Its Applications, 10(1), 385–414. https://doi.org/10.14257/ijsia.2016.10.1.35

[21] Hou, O. (2012). A Look at Google Bouncer. TrendLabs SECURITY INTELLIGENCE Blog. Retrieved from https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-googlebouncer/

[22] ISO/IEC. (2005). Iso/Iec 17799. Control, 1–170.

[23] https://www.incibe-cert.es/blog/unidos-las-ciberamenazas-information-sharing Unidos contra las ciberamenazas: Information Sharing. Antonio López. INCIBE. 6 de octubre de 2016 https://www.anomali.com/es/what-is-a-tip

[24] IOCs, una palabra de moda, un tema caliente. Pero ¿realmente conocemos sus capacidades? David Pérez. Panda Security. 25 de marzo de 2016, https://www.pandasecurity.com/spain/mediacenter/seguridad/iocs-y-sus-capacidades/

Indicadores de Compromiso Base de Datos Open, https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-tags/indicators-of-compromise (2019)

[25] Indicadores de Compromiso en la gestión de riesgos. Iker Sala Simón. Audea.com. 9 de julio de 2018

¿Qué es una plataforma de inteligencia contra amenazas (TIP)?. anomali.com https://www.audea.com/indicadores-compromiso-la-gestion-riesgos/

[26] Janosik, S. M. (2005). The Incident Object Description Exchange Format Status. NASPA Journal, 42(4), 1. https://doi.org/10.1017/CBO9781107415324.004.

[27] Jaramillo, G. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. Apuntes de Ciencia & Sociedad, 01(02), 167–171. https://doi.org/10.18259/acs.2011026

[28] Katz, J. (2010). Digital Signature, 197. https://doi.org/10.1017/CBO9781107415324.004

Mahindru, A., & Singh, P. (2017). Dynamic permissions based Android malware detection using machine learning techniques. 10th Innovations in Software Engineering Conference (ISEC), 202–210. https://doi.org/10.1145/3021460.3021485

[29] Lord, N. (2018). What are Indicators of Compromise? https://digitalguardian.com/blog/what-are-indicators-compromise#:~:text=Indicators of compromise (IOCs) are,malware infections%2C or other

[30] Martinez, A. (2014). La «otra manera» de identificar malware (/blog/indicadores-de-compromiso). Retrieved from https://www.incibe-cert.es/blog/indicadores-de-compromiso

[31] Naik, N., Jenkins, P., Savage, N., Yang, L., Naik, K., & Song, J. (2019). Augmented YARA Rules Fused with Fuzzy Hashing in Ransomware Triaging. 2019 IEEE Symposium Series on Computational Intelligence, SSCI 2019, 625–632. https://doi.org/10.1109/SSCI44817.2019.9002773

[32] Mendoza López, M. Á. (2015). Riesgos de seguridad en Android. Revista .Seguridad UNAM.

Retrieved from http://ru.tic.unam.mx:8080/tic/handle/123456789/1688

[33] Mieres, J. (2009). Ataques informáticos, Debilidades de seguridad comúnmente explotadas .

[34] Montala NSA en tu casa. Iván Portillo y Gonzalo González. HoneyCon 4ª edición. Noviembre de 2018. https://www.incibe-cert.es/blog/unidos-las-ciberamenazas-information-sharing

[35] Peñarredonda Jose Luis, 2015 LOS HUECOS DE SEGURIDAD EN MÓVILES MÁS TENEBROSOS DE LA HISTORIA. URL http://www.enter.co/chips-bits/seguridad/los-huecos-de-seguridad-en-moviles-mas-tenebrosos-de-la-historia/

[36] Rafa Hacker recomienda: Los mejores recursos en Threat Intelligence. Rafa Hacker. 29 de septiembre de 2017 https://rafanunez.info/rafa-hacker/rafa-hacker-recomienda-los-mejores-recursos-en-threat-intelligence/

[37] Rey, H., & Carlos, J. (2010). La correlación de eventos con fines de seguridad, 2010.

[38] R. Danyliw, The Incident Object Description Exchange Format, URL http://www.ietf.org/rfc/rfc5070.txt.

Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. Journal of Network and Computer Applications, 38(1), 43–53. https://doi.org/10.1016/j.jnca.2013.05.008

[39] Seo, S. H. Richard Struse, OASIS Cyber Threat Intelligence (CTI) TC, URL https://www.oasis- open.org/committees/tc_home.php?wg_abbrev=cti

[40] Sophisticated indicators for the modern threat landscape: an instruction to OpenIOC (2011).

Guia de Introducción a IOC y Open IOC

[41] Shabtai, A., Kanonov, U., Elovici, Y., Chanan, G., A, Suarez-Tangil, G., … IEEE. (2016). 2112). Andromaly: Malware Detection Framework for Android Devices. Journal of Intelligent Information Systems Evolution Detection and Analysis of Malware for Smart Devices Surveys Tutorials.

[42] SECURITY THREAT INFORMATION ANALYSIS, Modi, Shimon (Washington, DC, US) Schall, Stephen A. (Arlington, VA, US) 2018.

[43] Simón, M. (2014). Cómo funciona la seguridad en Android. Retrieved from https://rootear.com/android/seguridad-en-android

[44] Singh, L., & Hofmann, M. (2017). Dynamic Behavior Analysis of Android Applications for Malware Detection. 2017 International Conference on Intelligent Communication and Computational Techniques (ICCT), (2013), 1–7. https://doi.org/10.1109/INTELCCT.2017.8324010

[45] Somarriba, O., Zurutuza, U., Uribeetxeberria, R., Delosieres, L., & Nadjm-Tehrani, S. (2016). Detection and Visualization of Android Malware Behavior. Journal of Electrical and Computer Engineering, 2016(i). https://doi.org/10.1155/2016/8034967

[46] TECNÓSFERA. (2018). Android, el sistema operativo con más vulnerabilidades en 2017. Retrieved from http://www.eltiempo.com/tecnosfera/novedades-tecnologia/android-fue-elsistema-operativo-con-mas-vulnerabilidades-en-2017-167314

[47] Ericka Chicko wski 2013 Top 15 Indicators Of Compromise. Dark Reading https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647.

[48] Villa nova-Pascual, O. (2016). Malware en Android y medidas de prevención https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise. Retrieved from http://reunir.unir.net/handle/123456789/3622

[49] Wang, X., Zhang, D., Su, X., & Li, W. (2017). Mlifdect : Android Malware Detection based on

Zhdanov. Zhdanov, A. (2019). Generation of Static YARA-Signatures Using Genetic Algorithm. Proceedings - 4th IEEE European Symposium on Security and Privacy Workshops, EUROS and PW 2019, 220–228. https://doi.org/10.1109/EuroSPW.2019.00031

[50] Russell B. Brandom, R. “There are now 2.5 billion active Android devices”. 2019 https://www.theverge.com/2019/5/7/18528297/google-io-2019-android-devices-play-store-total-number-statistic-keynote)

[51] McAfee Threat Report 2021 ,

[52] Karspersky 2020 https://securelist.com/mobile-malware-evolution-2020/101029/

[53] Osorio Sierra A, Mateus M, Vargas H. Vol. 19, n.° 3, pp. 131-142, 2020, Revista UIS Ingenierías, Página de la revista: revistas.uis.edu.co/index.php/revistauisingenierias

[54] Yi Min Shum (2020) Situación Global Mobile 2020, https://yiminshum.com/mobile-movil-app-2020/

[55] Massachusetts Institute of Technology, 2021, http://appinventor.mit.edu/