Mundo Fesc E-ISSN: 2216-0388 P- ISSN: 2216-0353 Artículo Original

Spyware en Smartphone: Análisis Bibliométrico

Spyware in Smartphones: Bibliometric Analysis

Recibido: 22 de septiembre de 2024
Aprobado: 17 de diciembre de 2024
publicación: 1 de mayo del 2025

Forma de citar: P. S. Cabarico Gelvez, C. E. Pardo García, and J. M. Calixto Cely, "Spyware en Smartphone: Análisis Bibliométrico", Mundo Fesc, vol. 15, no. 32, pp. 165-180 May 2025, doi: 10.61799/2216-0388.1740

Carlos Eduardo Pardo García
Doctorado en Educación,
carlospardo@ufps.edu.co,
https://orcid.org/0000-0002-6804-0987,
Universidad Francisco de Paula Santander,
Cúcuta, Colombia.

José Martín Calixto Cely
Maestría en Administración de Proyectos,
mcalixto@ufps.edu.co,
https://orcid.org/0000-0003-2460-4346,
Universidad Francisco de Paula Santander,
Cúcuta, Colombia.

Pedro Sebastian Cabarico Gelvez
Estudiante de Ingeniería de Sistemas,
pedrosebastiancg@ufps.edu.co,
https://orcid.org/0009-0003-5002-4473,
Estudiante de la Universidad Francisco de Paula Santander,
Cúcuta, Colombia.

***Autor para correspondencia:**
E-mail: pedrosebastiancg@ufps.edu.co

Spyware en Smartphone: Análisis Bibliométrico

Resumen

Hoy en día, casi todo el mundo tiene un smartphone Android en el bolsillo. Y claro, con ese crecimiento explosivo también han aumentado los riesgos para la seguridad digital. Sobre todo por el tema del spyware, ese tipo de software espía al usuario. Este trabajo intenta entender cómo ha evolucionado la investigación científica sobre este problema en concreto. Para eso, se revisaron 30 artículos sacados de bases de datos como IEEE, ACM, Scopus y Google Scholar. Un estudio cualitativo, con herramientas como Bibliometrix y VOSviewer. Estas ayudaron a detectar patrones: qué temas son tendencia, quiénes investigan con quién, cómo se mueven las ideas. El periodo más movido fue entre 2015 y 2020. Un montón de publicaciones, sobre todo enfocadas en técnicas de detección con inteligencia artificial y machine learning. Estados Unidos y también Italia destacan como líderes en la producción científica. Aún hay problemas. Limitaciones técnicas, vacíos legales, muchas soluciones que no terminan de funcionar. Android es abierto y flexible, lo cual es genial para desarrolladores. Pero también lo vuelve más frágil frente a ataques. Se propone integrar la tecnología con ética, leyes, educación. Un enfoque más completo. Porque esto no es solo un problema técnico: es un tema de derechos, de privacidad. Y claro, los desarrolladores, las empresas, los gobiernos tienen que involucrarse más. Ya no basta con parches y apps de seguridad.

Palabras clave: Android, Bibliométrico, Malware, Spyware, Teléfonos inteligentes.

Carlos Eduardo Pardo García, José Martín Calixto Cely, Pedro Sebastian Cabarico Gelvez

Spyware in Smartphones: Bibliometric Analysis

Abstract

Nowadays, almost everyone has an Android smartphone in their pocket. And of course, with that explosive growth, digital security risks have also increased especially due to spyware, that type of software that spies on the user. This paper aims to understand how scientific research on this particular problem has evolved. To do so, 30 articles from databases such as IEEE, ACM, Scopus, and Google Scholar were reviewed. It was a qualitative study, using tools like Bibliometrix and VOSviewer. These helped identify patterns: which topics are trending, who is collaborating with whom, how ideas are spreading. The most active period was between 2015 and 2020. A large number of publications, mostly focused on detection techniques using artificial intelligence and machine learning. The United States and also Italy stand out as leaders in scientific production. Problems still remain technical limitations, legal gaps, and many solutions that don't quite work. Android is open and flexible, which is great for developers. But it also makes it more vulnerable to attacks. The proposal is to integrate technology with ethics, laws, and education in a more comprehensive approach. Because this is not just a technical issue: it's a matter of rights and privacy. And of course, developers, companies, and governments need to get more involved. Security patches and apps are no longer enough.

Keywords: Android, Bibliometric, Malware, Spyware, Smartphones.

Introducción

En seguridad informática, el spyware es una de esas amenazas silenciosas pero constantes. Es un tipo de software malicioso que se instala sin el consentimiento del usuario. Y una vez dentro, empieza a recopilar información personal de forma encubierta, vulnerando la privacidad, sí, pero también la integridad de los datos. Esta amenaza se ha vuelto especialmente preocupante en el mundo de los dispositivos móviles. Entre los sistemas operativos móviles, Android es el más afectado por esta amenaza. ¿Por qué? Bueno, según Martín et al. [1], su arquitectura de código abierto ha hecho que sea mucho más fácil distribuir apps maliciosas que parecen legítimas. Aplicaciones que aparentan ser legítimas, pero que ocultan comportamientos maliciosos. Muchas veces, estas aplicaciones se instalan gracias a técnicas de ingeniería social bastante sofisticadas y, una vez activas, pueden acceder a datos muy sensibles: desde registros de llamadas hasta ubicación en tiempo real, mensajes personales e incluso credenciales bancarias. El análisis de Martín muestra algo preocupante: los atacantes no solo usan trucos visuales o interfaces falsas. Van más allá. Usan metadatos y explotan permisos del sistema para esconder comportamientos maliciosos. Esto representa un desafío importante para los sistemas tradicionales de detección de malware.

Las medidas que ayudan a identificar malware en Android avanzan notablemente y logran el empleo de la inteligencia artificial y el aprendizaje automático para buscar patrones imprevistos y componentes sospechosos en aplicaciones. Sahs y Khan [2] destacan la importancia de los modelos de los aprendizajes supervisados para distinguir entre el software seguro y malicioso antes de la ejecución. Kaur et al. [3] amplían la perspectiva presentando el modelo basado en la inteligencia artificial, que evaluó precisamente las aplicaciones infectadas de spyware.

Dado lo grande que es el problema, este estudio busca analizar cómo ha evolucionado el conocimiento científico sobre el spyware en Android, usando un enfoque bibliométrico. Para eso, se revisaron 30 publicaciones recientes, sacadas de bases como IEEE, ACM, Scopus y Google Scholar. Además, se usaron herramientas como Bibliometrix y VOSviewer para hacer el análisis. La idea concreta de este artículo es echar un vistazo a la producción científica que hay sobre spyware en Android, pero enfocándose solo en artículos publicados en bases de datos accesibles en línea y de libre acceso. Así, se puede entender mejor qué se ha investigado y hacia dónde va el tema. En resumen, este artículo se propone dos cosas: rastrear qué se ha escrito —y cómo— sobre el tema en la literatura científica, y revisar qué patentes han intentado capturar o esquivar al escurridizo spyware.

Materiales y métodos

La información semántica sobre el ataque se obtuvo de plataformas como IEEE en inglés, ACM, Scopus y Google Scholar, utilizando la ecuación de búsqueda “TÍTULO-

ABS-KEY Android AND spyware" para encontrar artículos relevantes. Los documentos adquiridos fueron tratados con Bibliometrix, una herramienta informática que produce archivos tipo.bib para su uso en análisis bibliométricos. El análisis bibliométrico se resume en tres pasos básicos: colección de datos, análisis de datos en matemáticas y visualización de datos : para visualizar la parte importante del punto de vista. Esta técnica garantiza un examen sistemático y detallado del Campo de estudio y descubrimiento científico sobre el spyware en Android.

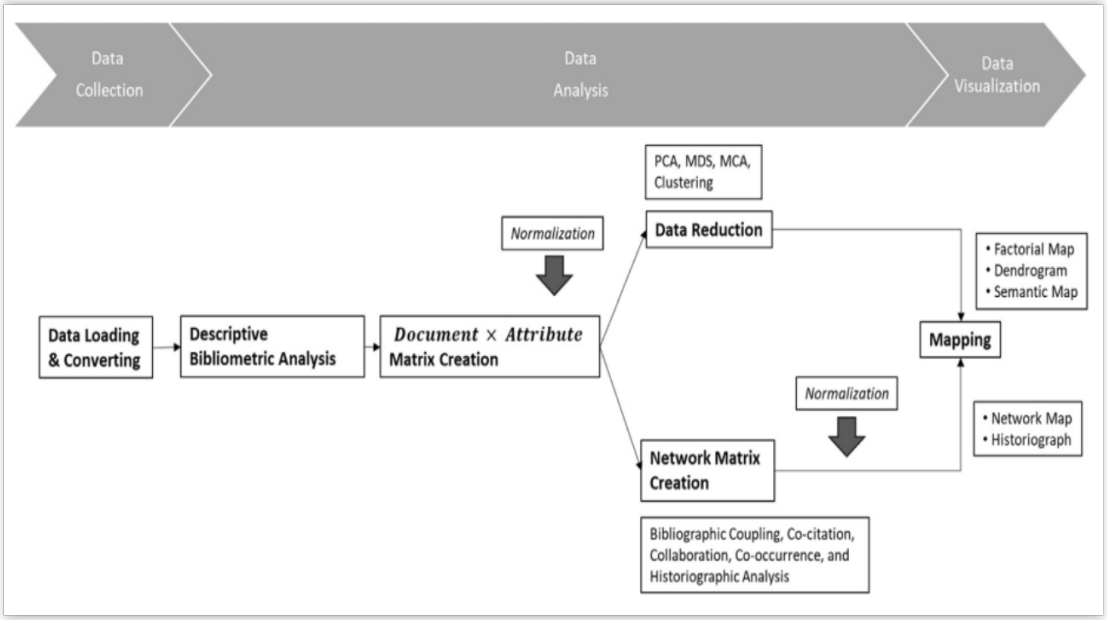

Figura 1. Pasos del Análisis Bibliometrix
Fuente: [4].

Se recurrió a Bibliometrix, una herramienta que no solo ordena datos, sino que los convierte en mapas: territorios temáticos donde las publicaciones científicas se agrupan como constelaciones. Además, se sumaron VOSviewer y Publish or Perish al equipo de navegación, especialmente útiles para explorar documentos en español.

Población y muestra de estudio

La población de estudio estuvo conformada por artículos en inglés recopilados de diversas bases de datos: ACM (11,815 documentos), IEEE (29 documentos) y Scopus (50 documentos), junto con 460 registros obtenidos a través de Google Académico. A partir de este conjunto, se seleccionó una muestra final de 30 estudios, determinada en función de su pertinencia temática según los criterios del investigador y su correspondencia con ecuaciones de búsqueda que incluían términos clave como Android, Malware, Spyware y Smartphones. La muestra quedó repartida así: 8 documentos de ACM, 7 de IEEE, 5 de Scopus todos en inglés y 10 en español, localizados a través de Google Académico.

Tabla I: Muestra seleccionada

Base de Datos Digital	Cantidad Seleccionada
ACM	*8*
IEEE	*7*
SCOPUS	*5*
Google Académico	*10*
Total	*30*

La Tabla I muestra cómo se compone esta muestra, enfocada en artículos sobre dispositivos móviles Android afectados por spyware. Se incluyeron textos en inglés y en español, entre ellos artículos científicos, tesis y algunos ensayos sacados de distintas bibliotecas digitales.

Resultados y discusión

El análisis bibliométrico, hecho con la herramienta Bibliometrix, permitió crear mapas que muestran la estructura general del corpus estudiado. Estos mapas evidenciaron puntos clave de los documentos, como las temáticas que predominan, las fuentes donde se publican y cómo se distribuyen en el tiempo los estudios. Este método ayudó a entender de forma más sistemática y ordenada el estado actual de la literatura, dando así una base fuerte para abordar el fenómeno que se investiga.

Análisis Bibliométrico de ACM

El análisis bibliométrico, hecho con la herramienta Bibliometrix, permitió crear mapas que muestran la estructura general del corpus estudiado. Estos mapas evidenciaron puntos clave de los documentos, como las temáticas que predominan, las fuentes donde se publican y cómo se distribuyen en el tiempo los estudios. Este método ayudó a entender de forma más sistemática y ordenada el estado actual de la literatura, dando así una base fuerte para abordar el fenómeno que se investiga.

Figura 2 Mapa de red de los temas principales de documentos de publicaciones científicas obtenidas de AC

Se evidencia que estos temas guardan una estrecha relación con el spyware y los mecanismos de detección. Asimismo, al examinar las fuentes de información de los documentos recopilados desde ACM a través de un mapa de clasificación de fuentes, se obtiene la representación visual mostrada en la siguiente figura.

Tabla II:

Mapa de los tipos de fuentes principales, para documentos y publicaciones científicas obtenidas de ACM

Fuente	N. de Documentos
ACM COMPUT. SURV.	*5*
PROCEEDINGS OF THE SECOND INTL. CONF.	*4*
PROCEEDINGS OF THE 2016 ACM WORKSHOP	*3*
PROCEEDINGS OF THE 2017 ACM ASIA CONF.	*3*
SIGSOFT SOFTW. ENG. NOTES	*2*
ANNUAL COMPUTER SECURITY CONF.	*2*
DIGITAL THREATS	*2*
INTERACTIONS	*2*
PROCEEDINGS OF THE 10TH ANNUAL CYBER	*2*
PROCEEDINGS OF THE 11TH ACM CONF.	*2*
PROCEEDINGS OF THE 15TH ACM ASIA CONF.	*2*
PROCEEDINGS OF THE 16TH INT. CONF.	*2*
PROCEEDINGS OF THE 17TH ANNUAL CONF.	*2*
PROCEEDINGS OF THE 18TH INT. CONF.	*2*
PROCEEDINGS OF THE 1ST ACM WORKSHOP	*2*
PROCEEDINGS OF THE 1ST INT. WORKSHOP	*2*
PROCEEDINGS OF THE 2016 INTERNET MEASUREMENT	*2*
PROCEEDINGS OF THE 2020 2ND ASIA PACIFIC	*2*
PROCEEDINGS OF THE 2020 9TH INTL. CONF.	*2*
PROCEEDINGS OF THE 29TH ACM JOINT MEETING	*2*

En consecuencia, se concluye que los documentos de ACM presentan una interconexión temática alineada con la naturaleza del estudio en desarrollo. Además, se destaca que sus fuentes de información son confiables, ya que provienen de publicaciones internacionales recientes, incluyendo conferencias internacionales, workshops, congresos y otros eventos académicos de relevancia, como se ilustra en la figura anterior.

Análisis Bibliométrico de IEEE

Al realizar un análisis bibliométrico de los documentos disponibles en la base de datos de la IEEE, se observa que los contenidos están mucho más relacionados con el tema investigado: Spyware en Smartphone. Utilizando el software Bibliometrix, se generó un mapa (mostrado en la figura 3) que destaca esta relación. Los trabajos científicos

encontrados en esta base de datos muestran una fuerte correlación con temas como Malware, Spyware, Android, Mobile Communication y Security, entre otros.

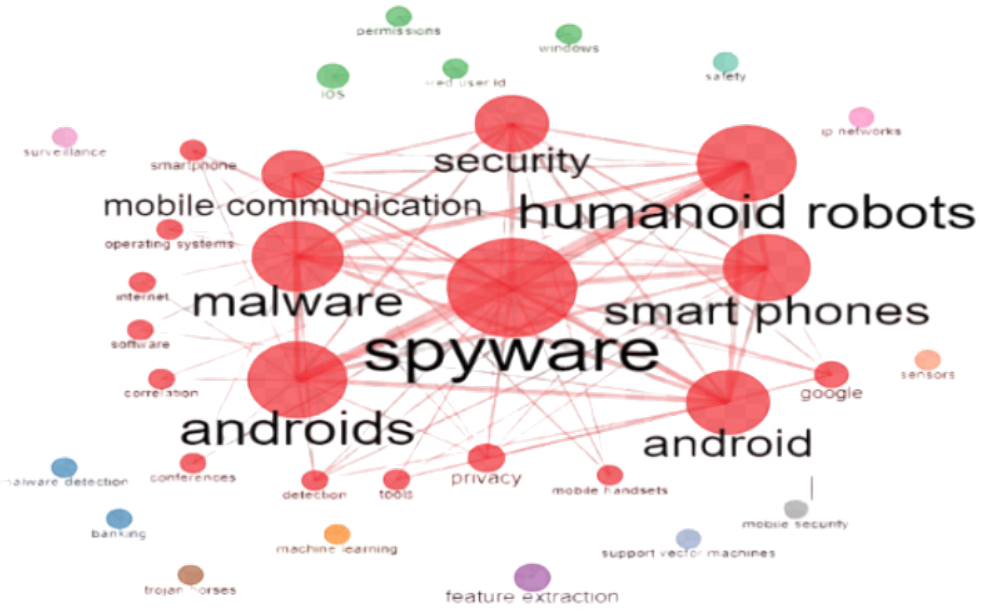

Figura 3 Mapa de red de ocurrencia de temas relacionados a la investigación sobre Spyware en Smartphone, en IEEE

Producción científica a lo largo del tiempo

Los primeros artículos sobre este tema aparecieron en 2012. Desde ahí, la producción científica fue creciendo poco a poco, hasta llegar a un pico en 2015. Luego, en 2016 y 2017, la cantidad de publicaciones disminuyó. Después, entre 2018 y 2021, hubo una especie de vaivén, con altibajos en el número de estudios publicados.

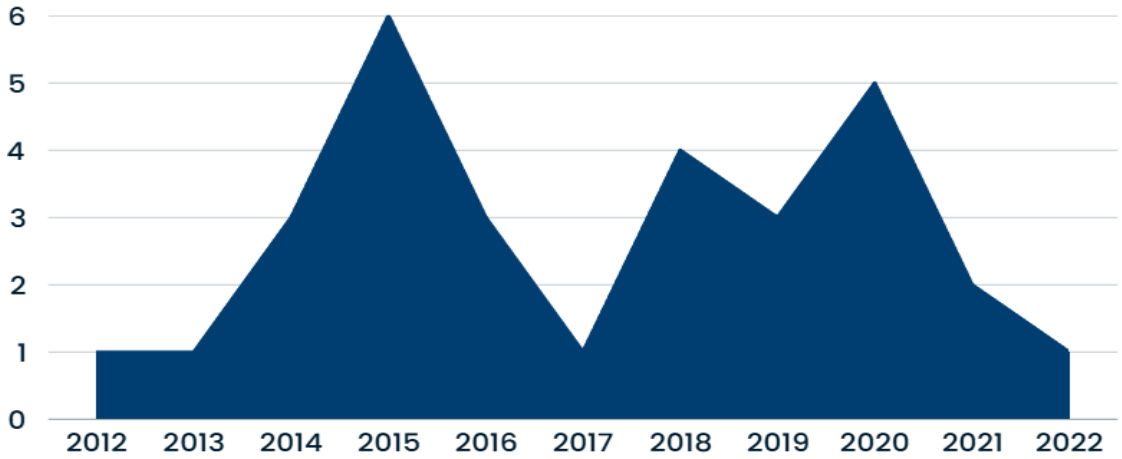

Figura 4 Gráfico informativo por años

Este comportamiento puede observarse con mayor claridad en la figura correspondiente. Al centrar el análisis en los años recientes, se identifican tres picos significativos de producción científica en 2015, 2018 y 2020, seguidos de una disminución notoria en

2022. Estos datos se visualizan en la Figura 4, generada mediante la herramienta Bibliometrix.

Análisis Bibliométrico de SCOPUS

Para realizar el análisis bibliométrico de los documentos relacionados con el tema de Spyware en Smartphones en la plataforma Scopus, se generó un mapa que destacó los temas de investigación más frecuentes y su interconexión. Los términos predominantes identificados en este análisis incluyen Android, Malware detection y Machine Learning. Estos conceptos están muy ligados al núcleo del estudio, porque hablan justo del enfoque principal de la investigación: detectar spyware en dispositivos móviles, especialmente en Android, usando técnicas avanzadas de aprendizaje automático — o sea, machine learning. Lo importante de esto viene por dos razones principales: primero, la enorme penetración que tiene Android a nivel global como sistema operativo móvil líder; y segundo, la complejidad creciente de las amenazas de spyware, que piden soluciones técnicas cada vez más innovadoras y efectivas. Por eso, este enfoque es clave para poder enfrentar el problema de forma eficiente. Ahora, en este contexto, se hizo un análisis de coautoría y temporalidad de las investigaciones, cuyos resultados se resumen en la Figura 5. Esa figura muestra quiénes son los autores más citados en el campo y en qué años hicieron sus contribuciones más importantes, lo que ayuda a identificar a los referentes clave y los momentos de mayor impacto en la producción académica sobre este tema.

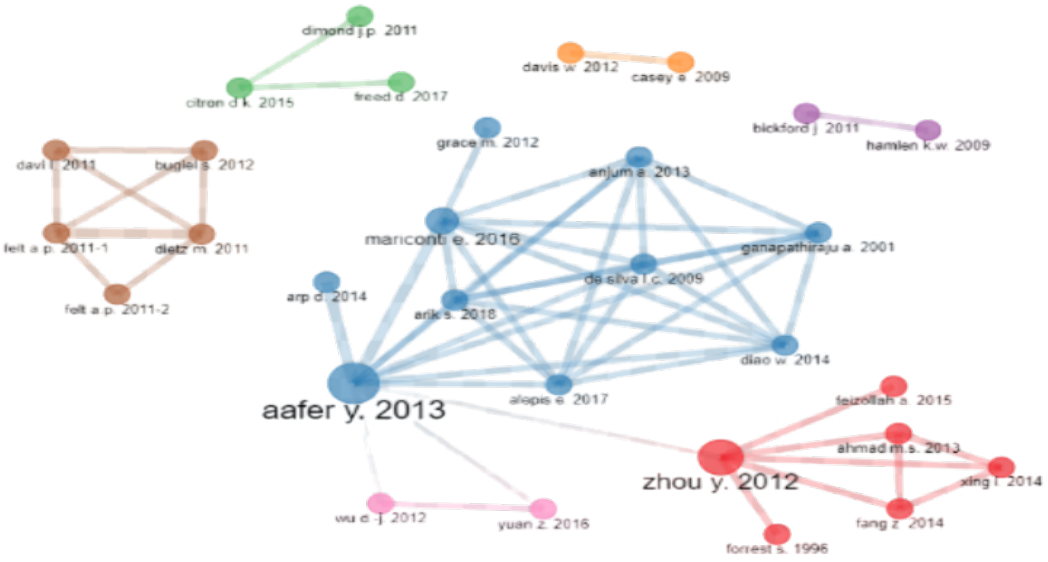

Figura 5 Mapa de red de autores relacionados y años de realización de sus investigaciones

Al meternos de lleno en el análisis de los autores que trabajan esta temática y de los años en que publicaron sus investigaciones, como se muestra en la Figura 5 pudimos identificar a los más citados y los momentos clave.

Se descubrió que las publicaciones más recientes, especialmente las que salieron entre 2015 y 2018, están fuertemente conectadas con investigaciones que se hicieron años antes, entre 2009 y 2013. Esa relación temporal sugiere una evolución constante, una especie de hilo que no se ha roto.

Pero, ¿qué países están realmente al frente de esta carrera científica? ¿Y qué los hace destacar sobre el resto? Bueno, según lo que encontramos en nuestro análisis bibliométrico y que se ve reflejado en la Tabla III Estados Unidos lidera con claridad. domina con su cantidad de publicaciones.

Tabla III: Mapa de colaboradores a nivel mundial

From	To	Frequency
Australia	*Canadá*	*1*
Canadá	*Singapore*	*1*
China	*Australia*	*1*
Germany	*Switzerland*	*1*
India	*Saudi Arabia*	*1*
Italy	*Germany*	*1*
Italy	*Morocco*	*1*
United Kingdom	*Morocco*	*1*
Usa	*Austria*	*1*
Usa	*Canadá*	*1*
Usa	*Israel*	*1*
Usa	*Italy*	*1*
Usa	*Korea*	*1*
Usa	*Morocco*	*1*
Usa	*Singapore*	*1*
Usa	*United Kingdom*	*1*

Análisis Bibliométrico de Google Académico

El análisis bibliométrico de documentos sobre spyware en smartphones, extraídos de Google Académico, permitió identificar investigaciones significativas que enriquecen el estudio documental del tema en los últimos años. Debido a que el formato de estos documentos impidió su procesamiento en la plataforma Bibliometrix, se recurrió al software VOSviewer y publish-or-perish para elaborar mapas bibliométricos.

Aunque no ha sido de gran fortaleza para el análisis bibliométrico de documentos en español. No obstante, el contenido de los documentos si fueron temas relacionados al estudio, y han sido relevantes. A continuación, se presentan algunos aportes de ellos. Para hacerles frente a los spywares, los usuarios de Android cuentan con algunas herramientas. Una de ellas es API Integrity [5], pensada para bloquear accesos no autorizados y frenar interacciones fraudulentas. Pero no se queda ahí. También hay investigaciones, como la de Arp et al. [6], que desarrollaron sistemas como Debrin,

enfocados en mejorar la detección de malware dentro de Android.

También está el caso que describe Rivera [7], desde Madrid, España, sobre Pegasus. Un spyware que marcó un antes y un después. Creado por NSO Group, este software fue capaz de hacer jailbreaks en iPhones y vulnerar sistemas que, en teoría, eran súper seguros. Pegasus podía acceder a audios codificados, leer mensajes cifrados, escalar privilegios, saltarse casi todas las barreras de protección. Este caso generó controversia en la comunidad internacional, suscitando debates técnicos y éticos.[8].

En Bucaramanga, Colombia, un par de investigadores Cardozo & Celis [9] se metieron de lleno en el lado oscuro de la seguridad móvil en Android. Android, como sistema operativo móvil más utilizado a nivel global, también presenta una alta tasa de ataques. Ransomware, troyanos, gusanos informáticos. ¿Por qué? Bueno, según su tesis, hay cuatro puntos críticos: fallas en el diseño del sistema, malos hábitos de los usuarios, errores de configuración y, además, límites en los protocolos de seguridad Y sí, Estas vulnerabilidades impactan tanto en la integridad del sistema como en la seguridad de los datos del usuario.

Mientras tanto, en otra región de Colombia, Manrique [10] realizó un estudio titulado “Análisis De La Seguridad De Smartphone Con Sistema Android”. Por ejemplo android 6.0 llegó a ocupar el puesto 26 en el ranking de CVE (Common Vulnerabilities and Exposures). Eso refleja una avalancha de vulnerabilidades que permiten desde el robo de información hasta ataques de ingeniería social, cortes en los servicios, e incluso manipulación de los datos almacenados.

Avanzando un poco más en el tiempo, en 2021, desde Quibdó, Chocó, Mena[11] presentó su estudio “Análisis De Riesgo De Seguridad En Los Dispositivos Móviles Personales Con Sistema Operativo Android”. Usando la metodología OPEN ANDROID SECURITY ASSESSMENT METHODOLOGY (OASAM) Esta permite evaluar con lupa cada rincón de seguridad en Android. Su conclusión aporta una perspectiva relevante, las actualizaciones del sistema no son solo para agregar funciones. También son una barrera defensiva, un escudo contra amenazas nuevas que aparecen todo el tiempo. Es decir, actualizar el sistema no es un capricho: es una necesidad de seguridad.

En el campo de la detección de spyware, Qabalin y Alkasassbeh [12], desde la Universidad de Tecnología Princess Sumaya, hicieron una propuesta bastante interesante. Armaron un conjunto de datos bien completo que cubre tres momentos clave: el tráfico normal de smartphones, el tráfico mientras se instala el spyware y el tráfico que se genera una vez que el spyware ya está operando en Android. Esta base les permitió entrenar modelos de detección, precisiones que van desde un 69% hasta un 93,2%. Bastante prometedor, sobre todo considerando que trabajaron con malware conocidos como UMbix, TheWiSPY y FlexiSPY. O sea, herramientas reales, no solo teóricas. Esto muestra que, aunque todavía hay margen para mejorar, se están dando pasos importantes para identificar mejor estas amenazas.

En Perú, Montenegro [13] exploró qué algoritmos de machine learning funcionan mejor para detectar malware en Android. Consiguió un rendimiento del 95,3% al clasificar tanto categorías como familias de malware.El estudio presenta resultados prometedores para futuras investigaciones. él mismo reconoce que es solo el comienzo. La idea es ampliar el análisis con más datos en futuras investigaciones, lo que podría afinar todavía más los modelos. En resumen, aunque el estudio fue limitado en escala, abre una puerta interesante para seguir mejorando la detección de amenazas en un sistema tan extendido como Android.

Finalmente, Ortega [14] se metió en un terreno un poco distinto: la forma en que nos comunicamos a través de los smartphones. Por un lado, resaltó las oportunidades, pero también fue claro con los riesgos. Habló de cómo los datos personales que guardamos, ya sea en el dispositivo o en la nube, están expuestos al espionaje y a la vigilancia, ya sea con intereses políticos o comerciales. Aun así, planteó algo interesante: que toda esa información podría usarse para mejorar la vida de las personas, no solo para vender más o controlar conductas.

Resultados

Se realizó un análisis detallado de documentos en bases de datos mediante un estudio bibliométrico de publicaciones en inglés. Este examinó autores, años y temas principales, generando una representación gráfica con Bibliometrix que destaca a investigadores como Chatterjee et al. [15] sobre privacidad y violencia en pareja, y Pierazzi et al. [16] sobre spyware en Android. IEEE es la fuente con mayor cantidad de estudios relevantes, identificaron familias de spyware como UaPush Pincer y AceCard, que roban datos o actúan como spyware bancario. Aunque estiman que el 68.5% de los ataques afectan a Android.

El spyware es una amenaza frecuente en Android debido a su código abierto y la rápida evolución del malware frente a defensas limitadas. Estudios indican que el 68.5% de los ataques de malware se dirigen a esta plataforma, incluyendo spyware que habilita ransomware o fraudes bancarios como AceCard [16], [17] mencionan fraudes por clics y troyanos bancarios, mientras Sowndarajan y Binu [18] señalan riesgos por permisos descuidados.

Se han desarrollado métodos como DroidSmartFuzzer [19] para reducir vulnerabilidades con pruebas de fuzz, y NADM [20], que usa redes neuronales con 90% de precisión. Zhang et al. [21] proponen inteligencia artificial contra spyware en asistentes de voz, y Wit et al. [22] abogan por detección dinámica con clasificadores como Random Forest.

Sin embargo, las técnicas actuales son limitadas. Shabtai et al. [23] crearon Andromaly, un sistema conductual para detectar malware, mientras Hu y Chen [24] presentaron

ShadowDroid, destacando la vulnerabilidad de Android (85-87% del mercado) por su apertura. En 2021, Yufei et al. reportaron un aumento del 27% en stalkwares. En Colombia, soluciones como DOSMELT y CreepRank no son definitivas.

Hu y Chen [24]sugieren que el spyware representa el 85-87% de los incidentes, evidenciando una creciente vulnerabilidad que requiere mejores medidas de seguridad.

Conclusiones

Se demuestra que la investigación sobre spyware en dispositivos Android creció bastante entre 2015 y 2020. Durante ese periodo, países como Estados Unidos e Italia marcaron la pauta en producción científica. Todo apunta a que el sistema operativo Android, con toda su apertura y flexibilidad, también abrió la puerta a una avalancha de amenazas. Sí, es un sistema que permite innovar, pero también lo hace especialmente vulnerable a ataques. Entre esos el spyware.

También se observó que las técnicas de detección han avanzado. Mucho. En especial aquellas que usan inteligencia artificial y análisis dinámico del comportamiento. Pero hay un detalle. Porque los atacantes no se quedan quietos. Sus técnicas evolucionan rápido. Y eso pone a prueba la eficacia de los sistemas actuales, dejando claro que aún nos falta. Faltan soluciones más completas. Más preparadas.

Entonces, se sugiere que las investigaciones futuras no solo se enfoquen en sistemas adaptativos que puedan reaccionar al instante ante nuevas amenazas. También deberían reforzar la educación en ciberseguridad para usuarios comunes. Y revisar, de manera crítica, si las políticas actuales de protección de datos realmente funcionan como deberían. Especialmente en este entorno tan cambiante.

Se concluye que combatir el spyware en Android no es tarea fácil. Se necesita trabajo conjunto, constante, y que venga tanto de la tecnología como de las instituciones y la sociedad en general. Solo así se podrán crear entornos digitales más seguros y más confiables.

Referencias

[1] Martín, I., Hernández, J. A., Muñoz, A., y Guzmán, A., «Android malware characterization using metadata and machine learning techniques», arXiv:1712.04402, 2017. [En línea]. Disponible en: https://arxiv.org/abs/1712.04402

[2] Sahs, J. y Khan, L., «A Machine Learning Approach to Android Malware Detection», presentado en European Intelligence and Security Informatics Conference, Denmark: IEEE, 2012, pp. 141-147. [En línea]. Disponible en: https://ieeexplore.ieee.org/

document/6298824

[3] Kaur, A., Lal, S., Goel, S., Pandey, M., y Agarwal, A., «Android Malware Detection System using Machine Learning», presentado en International Conference on Sustainable Computing, ACM, 2024. doi: 10.1145/3675888.3676049. [En línea]. Disponible en: https://dl.acm.org/doi/10.1145/3675888.3676049

[4] Aria, M. y Cuccurullo, C., «bibliometrix: An R-tool for comprehensive science mapping analysis», Journal of Informetrics, 11, n.º 4, pp. 959-975, 2017. [En línea]. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1751157717300500

[5] Android Developers Blog, «Google developers blog», 2023. [En línea]. Disponible en: https://developer.android.com/google/play/integrity?hl=es-419

[6] Arp, D. y et al., «Drebin: detección efectiva y explicable de malware para Android en su bolsillo», presentado en Network and Distributed System Security Symposium, 2014. [En línea]. Disponible en: https://www.ndss-symposium.org/ndss2014/ndss-2014-programme/drebin-effective-and-explainable-detection-android-malware-your-pocket/

[7] Rivera, A., Análisis de Malware en Android II, Tesis de grado, Universidad Complutense de Madrid, Madrid, 2021. [En línea]. Disponible en: https://eprints.ucm.es/id/eprint/74304/1/RIVERA%20LE%C3%93N%2084977_ALEJANDRO_RIVERA_LEON_Malware_en_Android_II_1398832_1568894276.pdf

[8] Román, A., Luna, V., Sarabia, R., Lechuga, A., Hernández, R., y Rodríguez, N., «Análisis ético de la información en el escándalo Pegasus». [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7237676

[9] Cardozo, C. y Celis, J., Estudio de Seguridad en Dispositivos Móviles con Sistema Operativo Android, Tesis de grado, Universidad Autónoma de Bucaramanga, 2021. [En línea]. Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/14400/2021_Tesis_Cristian_Fabian_Cardozo.pdf

[10] Manrique, C., Análisis de la seguridad de Smartphone con sistema Android, Tesis de grado, Universidad Abierta y a Distancia de Colombia, Ibagué, 2019. [En línea]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31570/93236941.pdf

[11] Mena, O., Análisis de riesgo de seguridad en los dispositivos móviles personales con sistema operativo Android, Tesis de grado, Universidad Abierta y a Distancia de Colombia, Quibdó, 2021. [En línea]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/48690/oemenaa-.pdf

[12] Qabalin, M., Naser, M., y Alkasassbeh, M., «Detección de spyware en Android

mediante el aprendizaje automático: un nuevo conjunto de datos», Sensors, 22, n.º 15, p. 5765, 2022. [En línea]. Disponible en: https://www.mdpi.com/1424-8220/22/15/5765

[13] Montenegro, V., Análisis comparativo de algoritmos de machine learning para detección de malware en aplicaciones Android, Tesis de grado, Universidad Señor de Sipán, Pimentel, 2022. [En línea]. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10059/Montenegro

[14] Ortega, H., «Smartphones opportunities and risks», vol. 15, n.º 1, pp. 109-140, 2022. [En línea]. Disponible en: https://www.researchgate.net/publication/360702780

[15] Doerfler, P., Chatterjee, R., Orgad, H., Havron, S., y Palmer, J., «The spyware used in intimate partner violence», 2018. [En línea]. Disponible en: https://nyuscholars.nyu.edu

[16] Pierazzi, F., Mezzour, G., Han, Q., Colajanni, M., y Subrahmanian, V., «Una caracterización basada en datos del spyware moderno de Android», ACM Transactions on Management Information Systems, 11, n.º 1, pp. 1-38, 2020. [En línea]. Disponible en: https://dl.acm.org/doi/fullHtml/10.1145/3382158

[17] Han, Q., Gan, Y., y Gao, Y., «Combinando el aprendizaje automático tradicional y la detección de anomalías», presentado en International Conference on Machine Learning Technologies, Roma, Italia: ACM, 2022. [En línea]. Disponible en: https://dblp.org/db/conf/icmlt/icmlt2022.html

[18] Sowndarajan, K. y Binu, B., «Android security issues and solutions», presentado en International Conference on Innovative Mechanisms for Industry Applications, 2017. [En línea]. Disponible en: https://www.researchgate.net/publication/318412307

[19] Hassan, M., Serageldin, A., y Salama, G., «Android spyware disease and medication», 2015. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/7435516

[20] Viet, N. y Thanh, P., «NADM: Red neuronal para malware de detección de Android», presentado en International Symposium on Information and Communication Technology, 2018. [En línea]. Disponible en: https://dblp.org/rec/conf/soict/DucG18.html

[21] Zhang, R., Chen, X., Wen, S., Zheng, X., y Ding, Y., «Using AI to attack VA», [En línea]. Disponible en: https://ieeexplore.ieee.org/document/8861099

[22] PanMan de Wit, J., Bucur, D., y Van Der Ham, J., «Detección dinámica de malware móvil», Digital Threats: Research and Practice, 3, n.º 2, pp. 1-24, 2022. [En línea]. Disponible en: https://dl.acm.org/doi/10.1145/3484246

[23] Shabtai, A., Yuvai, E., Chanan, G., y Uri, K., «Andromaly», Intelligent Information Systems, 38, n.º 1, pp. 161-190, 2012. [En línea]. Disponible en: https://link.springer.

com/article/10.1007/s10844-010-0148-x

[24] Hu, Che-Chun y Chen, Yi-Ming, «Análisis dinámico de malware de Android», presentado en International Conference on Big Data and Computing, 2020. [En línea]. Disponible en: https://dl.acm.org/doi/10.1145/3418688.3418694