THE SEGURANDO: "Ethical Hacking Techniques" and "Android Security"

Abstract. Currently, mobile device security is critical due to the volume of sensitive information processed and the vast array of attack vectors (numbering in the millions as of 2025). Therefore, this research—utilizing ethical hacking techniques applied to the Android 9.0 Pie operating system—seeks to identify structural weaknesses and propose effective mitigation mechanisms.
The research was conducted within a virtualized simulation environment, implementing social engineering tactics and remote access malware via Command and Control (C&C) infrastructures to assess malicious software impact. Additionally, the study validates the feasibility of keystroke injection attacks leveraging Human Interface Device (HID) techniques.
To analyze the mechanisms of unauthorized data exfiltration, the modification of critical system settings, and the bypass of Android's native detection layers, both static and dynamic application analysis were performed.
The analysis identified security gaps in the system's interaction with peripherals and in the permission management of infected applications. This demonstrated the technical viability of complex attacks using open-source tools, analyzing the results in relation to existing protection measures and proposing new security layers.
This work provides a technical perspective aimed at raising awareness of current risks, highlighting the importance of offensive security practices to increased end-user defense and contributing to the resilience of mobile systems against emerging threats.

Keywords: Ethical Hacking, Android Operating System, HID, C&C.

THE SEGURANDO: "Técnicas de Hacking Ético" y "Seguridad en Android"

Resumen. Actualmente, la seguridad en dispositivos móviles es crítica debido al volumen de información sensible que procesan y a la gran cantidad de vectores de ataque (millones en 2025). Por lo tanto, este trabajo a través de técnicas de hacking ético aplicados al sistema operativo Android 9, busca identificar debilidades estructurales y proponer mecanismos de mitigación efectivos.
La investigación se desarrolla en un entorno de simulación virtualizado, donde se aplicaron técnicas de ingeniería social, y malware orientado al acceso remoto en infraestructuras de Comando y Control (C&C) evaluando el impacto de software malicioso. Además, validar la viabilidad de inyección de pulsaciones basado en la técnica de Human Interface Device (HID).
Para comprender la capacidad de cómo se logra la exfiltración de datos y la modificación de configuraciones críticas, sin el consentimiento del usuario,

como así también la evasión de los mecanismos de detección nativos de Android, se implementó análisis dinámico y estático de las aplicaciones.
En el análisis se identificaron brechas de seguridad en la interacción del sistema con periféricos y en la gestión de permisos de aplicaciones infectadas, visualizando la viabilidad técnica de ataques complejos con herramientas de código abierto, correlacionando los hallazgos con medidas de protección existentes y proponiendo nuevas capas de seguridad.
Este trabajo aporta una visión técnica que busca concientizar sobre los riesgos actuales, remarcando la importancia de las prácticas de seguridad ofensiva para robustecer la defensa de los usuarios finales, contribuyendo al fortalecimiento de la resiliencia de los sistemas móviles frente a amenazas emergentes.

Palabras clave: Hacking Ético, Sistema Operativo Android, HID, C&C.

1 Introduccion

En 2025, se registran más de 3.9 mil millones de usuarios del sistema operativo Android, convirtiéndolo en el sistema operativo móvil más utilizado (72.55%) (Kumar, 2025), a través de diferentes dispositivos que abarcan teléfonos celulares, smart tv, dispositivos IOT (Internet of Things), etc. Sin embargo, las amenazas se han incrementado, dado que el 97% correspondiente al malware móvil es para el sistema operativo Android y se registró un aumento del 150% de ataques malware troyanos bancarios en relación al 2024 según lo refleja Kaspersky (Nilesh, 2026) (Kivva,2026), mientras que en el 2026 AV-Test detectó más de 29 Millones de aplicaciones no deseadas y 37 Millones de malware (Av-Atlas,2026).
Los malware troyanos tienen diferentes usos: permitir que los dispositivos sean parte de una botnet (Kumar, 2025), robo de dinero o datos personales, acceso remoto (RAT) que pueden escalar logrando el control total del dispositivos.
Los ciberataques, afectan de diferente manera a los usuarios de dispositivos móviles, desde el robo de identidad, sustracción de datos sensibles, pérdida de dinero, invalidación del dispositivo hasta llegar a afectar a entornos que rodean a ese usuario, como lo sería la red de una empresa, red hogareña, red industrial, etc. Aprovechando generalmente los sectores más vulnerables, por ejemplo personas de tercera edad o niños que tienen cada vez más acceso a dispositivos móviles y son más susceptibles a ser víctimas de los ataques a sus dispositivos.
Por lo tanto, surge la necesidad de estudiar está problemática que incluye desde el análisis de vulnerabilidades de este sistema, reconocimiento de técnicas, tácticas y herramientas de ciberataque, identificación de tipos de malware y su impacto, mecanismos de protección del sistemas Android, así como el hardware requerido, todo esto enfocado bajo el aprendizaje de la metodología de hacking ético , lo que permite desarrollar el conocimiento necesario para mejorar la protección del sistema operativo Android (Drake et al,2014) (Han et al,2024) (Asmitha et al,2025) (Scarfone et al.,2008) (Thomas, J ,2024).

2 Desarrollo

Para aprender sobre la robustez y la arquitectura de Android se utilizaron dos técnicas de ataque: aplicaciones maliciosas y ataques HID. Siguiendo el lineamiento hacking ético se trabajó en un entorno controlado, permitiendo auditar el comportamiento del sistema e identificar vulnerabilidades que un atacante podría explotar para comprometer la integridad, confidencialidad y disponibilidad de la información almacenada en el dispositivo (Cano, 2013).
Se realizaron diferentes pruebas, en diferentes escenarios para observar los resultados:

- En dispositivo real XIAOMI Mi A1 con un sistema operativo nativo de Android versión 9 que dispone de un antivirus integrado.
- En un entorno virtualizado con sistema operativo android 9
- En un dispositivo real Redmi Note 9 pro con un sistema operativo nativo Android 12 y capa de personalización MIUI versión 14 y dispone de un antivirus integrado propio de Xiaomi. Con y sin ADB (Android Debug Bridge) activado.

2.1 Aplicaciones maliciosas e infraestructuras de Comando y Control (C&C)

El objetivo principal fue demostrar la viabilidad de tomar el control remoto total de un dispositivo tras la ejecución inadvertida de una aplicación comprometida. La técnica consistió en establecer una infraestructura de Comando y Control (C&C) a través de una conexión inversa (*reverse_tcp*), la cual permite al atacante administrar el celular a distancia, extraer información sensible y denegar servicios evadiendo las restricciones de seguridad del sistema.
Se utilizó ingeniería social para efectuar un ataque de phishing el cual convencería al usuario a instalar una aplicación maliciosa, inyectada con un *backdoor* en el archivo APK legítimo, utilizando software de código abierto:

- **TheFatRat:** Utilizada para automatizar la inyección del código malicioso en la aplicación original y generar el *payload* de la conexión inversa.
- **Apktool:** Herramienta empleada para aplicar ingeniería inversa, que desensambla los binarios de la aplicación a código legible para integrar el *backdoor* y, posteriormente, reconstruir el paquete final (https://apktool.org/)
- **Apksigner:** Para firmar digitalmente el APK resultante (herramienta oficial de android), garantizando que Android valide la firma y permita la instalación del software (https://source.android.com/docs/security/features/apksigning).
- **Metasploit Framework:** Plataforma usada para inicializar el estado de escucha (listener) en el servidor atacante y gestionar la sesión remota mediante el componente Meterpreter, lo que habilita la post-explotación del sistema (https://docs.rapid7.com/metasploit/msf-overview/).

Al momento de instalar una aplicación modificada, hubo distintos resultados: (1) Android 12 no dejaba instalarlo, no por detectar la modificación sino por una mala formación del manifest al momento de compilar, debido a la incompatibilidad de FatRat con las nuevas versiones de apps, luego de decompilar la aplicación, resolver el inconveniente y compilarla nuevamente esta aplicación quedó lista para instalarse sin inconvenientes en el celular, (2) los dispositivos reales sin ADB, detectaron pero no bloquearon ni eliminaron la aplicación maliciosa, provocando que mediante algunas acciones permitidas del sistema se lograra su instalación cabe aclarar que

entre las dos versiones de Android se observa diferencia gráfica en los permisos otorgados, (3) en Redmi Note 9, sin tarjeta SIM y sin cuenta MI de xiaomi y con ADB limitado para depuración o instalación de aplicaciones, se requirió desactivar (sin requisito previo) la opción “optimización MIUI” para que el sistema permita la instalación de cualquier app por ADB de forma directa y sin avisos, y (4) haciendo uso del entorno virtualizado con permisos de root la instalación se realizó sin inconveniente y se pudo observar mediante la herramienta adb, una gran cantidad de socket abiertos al servidor C&C demostrando que el malware utiliza hilos independientes para diferentes tareas y el sistema no genera ninguna alerta.
Una vez accedido al celular desde el C&C y con los permisos dados se logró: descargar archivos desde la carpeta “Downloads”, grabar audios utilizando el micrófono del dispositivo aunque de muy corta duración, realizar capturas de la pantalla del celular, ver la lista de aplicaciones e información de la arquitectura del android, revisar si está rooteado, ver y descargar los contactos, y descargar los SMS.
Si el celular estuviera rooteado se pueden realizar muchas más operaciones ya que se puede incluso solicitar permisos de root desde la aplicación.

2.2 Ataque HID (Human Interface Device)

El objetivo fue evaluar la vulnerabilidad de Android 9 ante la inyección automatizada de comandos a través de puertos físicos, aprovechando la confianza implícita que el sistema operativo otorga por defecto a los periféricos de entrada USB, lo que permite al atacante realizar acciones que pueden comprometer el sistema sin requerir interacción activa ni consentimiento por parte de la víctima. (Nicho et al, 2025).
Para la ejecución técnica del ataque, se utilizó una placa microcontroladora Raspberry Pi Pico W equipada con el firmware AtomDucky, la cual actuó como el dispositivo atacante, que se conectó físicamente al Xiaomi Mi A1 mediante un adaptador OTG.
El microcontrolador fue reconocido de forma automática como un teclado legítimo y a través de la emulación de pulsaciones de teclas a velocidades sobrehumanas (usando un lenguaje basado en etiquetas) se instaló la aplicación maliciosa.

3 Conclusiones y trabajos futuros

Este trabajo de investigación aún se encuentra en desarrollo, por lo tanto no todas las pruebas han sido completadas.
Las pruebas realizadas permitieron validar el cumplimiento de los objetivos planteados.
Sin embargo, la activación del modo ADB no es directa, con una campaña de phishing sería difícil, pero usando el ataque HID se lograría sin conocimiento del usuario.
La técnica HID mostró que el sistema es bastante frágil cuando se trata de gestionar la conexión con dispositivos HID, ya que no dispone de un mecanismo de autenticación de dispositivos robusto que verifique si ese hardware es legítimo, permitiendo que un microcontrolador programable pueda emular un teclado o un mouse y de esta forma controlar el dispositivo (alterar la configuración, instalar aplicaciones, etc.) de manera válida para el sistema con la posibilidad de ser indetectable por el usuario.

De este trabajo se logra visualizar una superficie de ataque muy seria de fácil ejecución, que representa un riesgo real, en ocasiones no contemplada, asociada a la interacción entre el hardware y el sistema operativo.
En cuanto al futuro para este trabajo, resta completar las pruebas pendientes y profundizar en el impacto que tiene mantener activas las conexiones C&C y la ejecución de posibles comandos por HID. Además, señalar recomendaciones para mitigar las vulnerabilidades identificadas, por ejemplo: valorar soluciones que permitan al sistema operativo detectar patrones de pulsación anormales, bloquear las entradas HID que no pasen por una verificación previa de forma temporal o identificar el dispositivo conectado.

Referencias

Kumar, N (2025). Android Statistics: Market share, usage & facts. DemandSage. https://www.demandsage.com/android-statistics/

Nilesh Jain. (20 de febrero de 2026). *Mobile App Security Testing in 2026: Statistics, OWASP Threats, and What It Costs to Get It Wrong.* Vervali. https://www.vervali.com/blog/mobile-app-security-testing-in-2026-statistics-owasp-threats-and-what-it-costs-to-get-it-wrong

Kivva Anton. (4 de marzo de 2026). Virología móvil 2025. Securelist. https://securelist.lat/mobile-threat-report-2025/100828/

AV-Atlas. (2026). Malware statistics. AV-Test. https://portal.av-atlas.org/malware/statistics

Drake, J., Oliva P. , Lanier, Z., Mulliner, C., Ridley, S. y Wicherski, G. (2014). *Android Hacker's Handbook*. John Wiley & Son.

Han Q, Mandujano S., Porst S., Subrahmanian V., Deep Tetali S. y Xiong Y.. (2024). *The Android Malware Handbook.* No starch press.

Asmitha K.A., Vinod P., Rafidha Rehiman K.A., Raveendran N. y Conti M. (2025). Android malware defense through a hybrid multi-modal approach. *Journal of Network and Computer Applications*. Volume 233. 1084-8045. ISSN 104035. https://doi.org/10.1016/j.jnca.2024.104035.

Scarfone, K., Souppaya M., Cody A, y Orebaugh A. (2008). *Technical Guide to Information Security Testing and Assessment* (NIST Special Publication 800-115). National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Thomas, J. (2024). *Android Ethical Hacking: Tools, Techniques, and Security Strategies*. ISBN: 9789349075016, 9349075016.

Cano, J. J. (2013). *Seguridad informática y forense*. Alfaomega.

Nicho, M., y Sabry, I. (2022). Threat and Vulnerability Modelling of Malicious Human Interface Devices. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics*, 21, 241-247. ISSN: 2602-3199. https://www.researchgate.net/publication/366755114