# Mobile Threat Defense (MTD). Un acercamiento teórico.

1st Nicolás Ariza Barbosa, 2nd Mateo Olaya Garzón, 3rd Santiago Andrés Rocha
*Escuela Colombiana de Ingeniería Julio Garavito, Bogotá, Colombia*
nicolas.ariza@mail.escuelaing.edu.co, mateo.olaya@mail.escuelaing.edu.co,
santiago.rocha-c@mail.escuelaing.edu.co

***Resumen*—El artículo aborda la importancia de la seguridad móvil en un mundo donde los dispositivos móviles son esenciales para la vida cotidiana con Mobile Threat Defense (MTD), una estrategia integral para proteger la ciberseguridad en dispositivos móviles. El MTD se presenta como una solución sofisticada que no solo detecta y responde a amenazas móviles, sino que también previene riesgos al identificar vulnerabilidades. Además, se proporciona un contexto histórico sobre la evolución de las amenazas cibernéticas móviles y se subraya la necesidad de concienciar a los usuarios sobre la seguridad en dispositivos móviles en un mundo cada vez más interconectado. El artículo enfatiza el papel esencial del MTD en la protección de datos y la privacidad en dispositivos móviles, así como la importancia de mantenerse al tanto de las amenazas cibernéticas en constante evolución.**

***Index Terms*—Mobile Threat Defense, Seguridad Móvil, Amenazas Cibernéticas, Seguridad Empresarial, Vulnerabilidad, Dispositivos Móviles.**

## I. Introducción

La sociedad contemporánea esta estrechamente relacionada con las últimas tecnologías de vanguardia y se puede decir que se están asentando para no irse jamas. Una de estas tecnologías son los dispositivos móviles, los cuales, han redefinido la cotidianidad permitiendo realizar múltiples operaciones destinadas a fines tales como comunicación, trabajo y entretenimiento. A su vez, la propagación de estos aparatos también trajo consigo un disparo considerable de amenazas cibernéticas. Los usuarios ahora se enfrentan a riesgos que ponen en peligro sus datos personales, privacidad e identidad.

En respuesta a ello, se ha creado el **MTD (Mobile Threat Defense)** entendiéndose como un conjunto de estrategias y tecnologías destinadas a proteger los pilares de la ciberseguridad en los dispositivos móviles. En este documento se detallara la importancia, técnicas, contexto histórico, soluciones y beneficios ofrecidos al ser implementado este componente.

Comprender y aplicar estos términos es vital teniendo en cuenta que los dispositivos móviles se han convertido en puertas de entrada valiosas a la vida digital de las personas y las empresas. Con este estudio se espera arrojar luz sobre este campo en constante evolución para así enfrentar con confianza los desafíos de seguridad móvil del siglo XXI.

## II. Marco Teórico

### *II-A. ¿Qué es?*

La defensa contra amenazas móviles (Mobile Threat Defense, MTD) es una protección de seguridad sofisticada y dinámica contra amenazas cibernéticas dirigidas a dispositivos móviles.


Figura 1. Ejemplo de MTD [3]

El MTD debe contemplar todos los ataques posibles diseñados para dispositivos móviles. Así, estas herramientas los escanean para encontrar malware, ataques de día cero o conexión a dominios sospechosos. También, avisan sobre posibles suplantaciones de identidad o phishing. Las herramientas pueden bloquear el acceso a las páginas ya catalogadas como de phishing móvil o alertar de su acceso. Pero el Mobile Threat Defense no solo sirve para actuar en cuanto se den esos ataques, sino también para prevenir, es decir, para reducir el riesgo. Así, estas herramientas avisan de vulnerabilidades que encuentran para que las empresas actúen antes de que sea peor. De hecho, estas pueden hacer auditorías periódicas para comprobar el riesgo de los dispositivos móviles que tienen sus empleados.

### *II-B. Contexto Histórico*

- **2004**: Fuimos testigos del primer virus móvil, un gusano llamado “Cabir”, cuyo blanco fueron los teléfonos Symbian utilizando el protocolo push Bluetooth OBEX.

- **2009**: Dos gusanos (“Ikee” y “Duh”) atacaron iPhones liberados al aprovecharse de una contraseña codificada de forma rígida en sshd.
- **2010**: El primer malware de Android llamado “FakePlayer” generó sumas de dinero mediante el envío de mensajes SMS a Rusia.
- **2011**: Google Play sufre el ataque proveniente de una gran cantidad de aplicaciones maliciosas.
- **2012**: Un bot bancario ya existente logró adaptarse para Android y robó datos de autenticación de transacciones móviles.
- **2013**: El malware de Android se oculta como una aplicación real mediante la vulneración de la validación de certificados.
- **2014**: Las aplicaciones bancarias falsas se instalan en dispositivos Android cuando estos se conectan a una PC vulnerada.
- **2015**: Otro virus de Android envió correos no deseados a contactos telefónicos con mensajes que contenían un enlace para instalar malware con la apariencia de una aplicación de recompensas de Amazon.
- **2016-2020**: Los ataques móviles continúan evolucionando y creciendo en cantidad y gravedad. La seguridad en dispositivos móviles adquiere más importancia que nunca.

## III. Uso y Aplicaciones

### *III-A. ¿Cómo funciona?*

Según Gartner [2], debido a que el malware móvil debe eludir o deshabilitar los controles integrados del dispositivo, MTD se centra en identificar indicadores de compromiso y señalar comportamientos anormales. Gartner identifica cuatro opciones de implementación clave para MTD:

- **UEM Integrado**: La inscripción y la implementación de MTD se facilitan a través de una solución UEM, que también gestiona la corrección.
- **Independiente (en el dispositivo)**: Un cliente MTD se implementa en dispositivos no administrados o no registrados.
- **Independiente (basado en proxy)**: El cliente MTD generalmente se implementa localmente y desvía todo el tráfico de la red a través de un motor de análisis para evaluar los indicadores de compromiso.
- **SDK/integrado**: MTD protege la aplicación en lugar del dispositivo en el que está instalada, escaneando cualquier actividad que pueda hacer que la aplicación sea insegura.

### *III-B. ¿Cómo se despliega?*

Para desplegar un MTD, la empresa decide si los empleados se descargan la app en una store o si la envían por correo electrónico o SMS para instalarla. Otra opción es apostar por una solución que venga integrada con el EMM. En este caso habrá que comprobar el nivel de integración de esta plataforma con la solución que tengamos previsto usar En cualquier caso, la mayoría de los productos de MTD se implementan a través de la nube. Estos servicios se pueden instalar en miles de teléfonos en menos de un día.

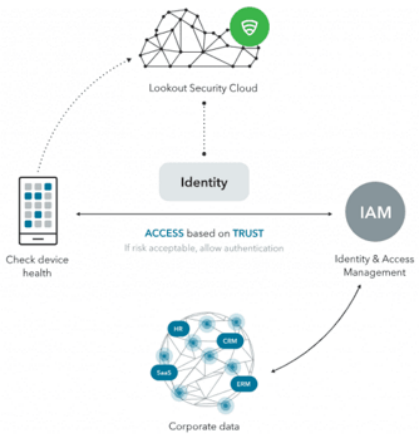


Figura 2. Ejemplo de Despliegue [3]

### *III-C. Beneficios*

- Adopción más sencilla de políticas de ”Bring Your Own Device”(BYOD).
- Monitoreo de amenazas móviles en las capas de dispositivo, red y aplicación sin agregar sobrecarga de SecOps.
- Protección y visibilidad de toda la flota móvil de una organización.
- Mitigación de amenazas comunes como los ataques de phishing.
- Respuesta más rápida a las amenazas. La solución de MTD impedirá que los ataques se conviertan en problemas graves.
- Integración con soluciones MDM/UEM/MAM que permite alertas de amenazas y remediación basadas en políticas existentes.
- Cumplimiento normativo. Son sistemas de seguridad para empresas que garantizarán que los datos confidenciales de la organización tengan la protección adecuada, estén donde estén.

### *III-D. Estadísticas de Amenazas Móviles*

En la figura 3 es posible evidenciar el número de paquetes de instalación detectados entre los años 2019 y 2022. En 2022 se detectaron 1.661.743 paquetes de instaladores maliciosos móviles, 1.803.013 menos que el año anterior. [4] 2022 la mayor parte de los ataques a usuarios de móviles fueron perpetrados por malware (67,78 %).

En la figura 4 se evidencia el aumento en la proporción de ataques que utilizan aplicaciones publicitarias (Adware) y aplicaciones de la clase RiskWare: 26,91 % (frente al 16,92 % en 2021) y 5,31 % (frente al 2,38 % en 2021), respectivamente. [4]

Finalmente, en la figura 5 Vemos cómo dos tercios de todos los troyanos bancarios detectados eran representantes de la familia Trojan-Banker.AndroidOS.Bray (66,40 %), que ataca principalmente a usuarios de Japón. La familia Trojan-Banker.AndroidOS.Fakecalls ocupa el segundo lugar (8,27 %) y Trojan-Banker.AndroidOS.Bian (3,25 %) ocupa el tercer lugar. [4]

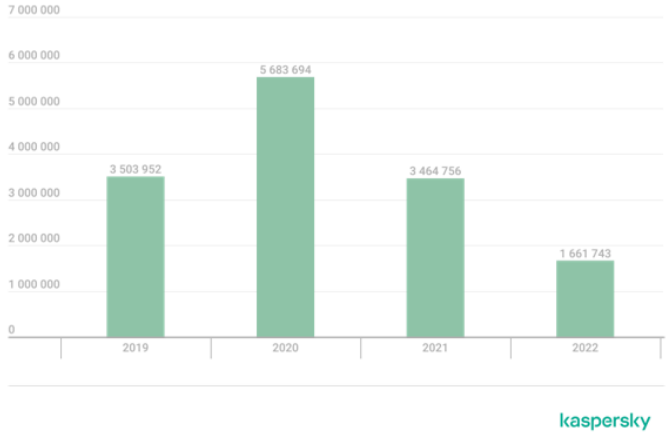


Figura 3. Número de paquetes de instalación detectados, 2019-2022 [4]

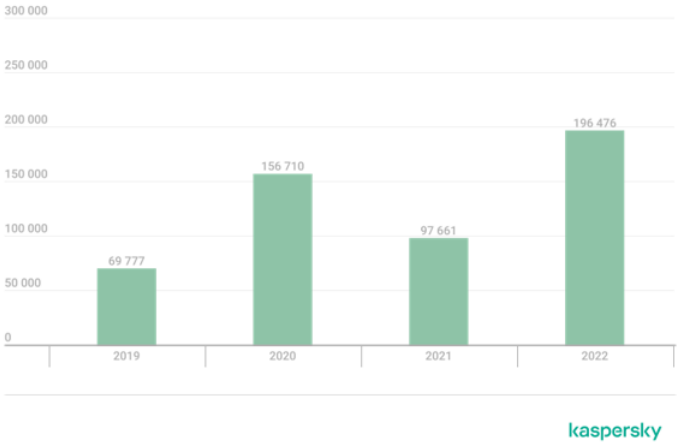


Figura 5. Número de paquetes instaladores de troyanos bancarios móviles detectados por Kaspersky, 2019-2022 [4]

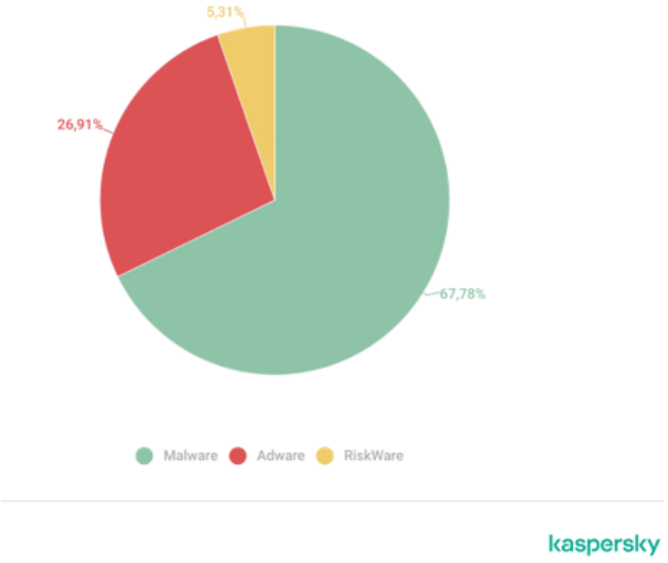


Figura 4. Distribución de los ataques por tipo de software utilizado, 2022 [4]

La información presentada en este fragmento destaca la importancia crítica del Mobile Threat Defense (MTD) en la protección de dispositivos móviles. La disminución en el número de paquetes de instaladores maliciosos entre 2019 y 2022, a pesar de que aún se detectaron más de un millón en 2022, muestra que las amenazas cibernéticas en dispositivos móviles siguen siendo una preocupación significativa. Además, el aumento en la proporción de ataques utilizando aplicaciones publicitarias y aplicaciones de riesgo resalta la necesidad de una defensa sólida contra amenazas móviles. Estos datos subrayan la importancia de implementar MTD para detectar y prevenir ataques, protegiendo así la seguridad y la privacidad de los usuarios de dispositivos móviles en un entorno donde el malware móvil sigue siendo una amenaza relevante.

## IV. Conclusiones

- Las amenazas cibernéticas suelen centralizarse hacia equipos de computo sofisticados (computadoras, laptops, servidores etc.) dejando de lado tecnologías cotidianas tan importantes como lo son los dispositivos móviles. La concienciación referente a la ciberseguridad en estos aparatos es pobre y debería recibir un mayor foco de atención por parte de los usuarios.
- El artículo resalta la importancia de una estrategia de seguridad móvil integral por medio de Mobile Threat Defense (MTD) como un componente esencial. Esto subraya la necesidad de proteger los dispositivos móviles en un mundo cada vez más conectado.
- El artículo proporciona un contexto histórico sobre la evolución de las amenazas cibernéticas móviles, desde los primeros virus móviles hasta los desafíos actuales, destacando la necesidad de soluciones de seguridad móvil.
- Describimos cómo funciona el MTD, centrándonos en la identificación de indicadores de compromiso y comportamientos anormales. También discutimos las opciones de implementación, incluyendo la integración con soluciones UEM y la implementación basada en la nube.
- El artículo destaca las razones para usar MTD, incluyendo la creciente amenaza de ataques cibernéticos móviles, la adopción de políticas BYOD y los desafíos de seguridad relacionados con el trabajo remoto.

## Referencias

[1] Rvega (2022) Seguridad en Dispositivos Móviles (MTD), Check Point Software ES. Available at: https://www.checkpoint.com/es/cyber-hub/what-is-mobile-threat-defense-mtd/ (Accessed: 17 September 2023).
[2] ¿Qué es MTD (mobile threat defense)? (no date) SEIDOR. Available at: https://www.seidor.com/blog/mtd-que-es (Accessed: 17 September 2023).
[3] Mobile threat defense (MTD) (no date) BlackBerry. Available at: https://www.blackberry.com/us/en/solutions/endpoint-security/mobile-threat-defense (Accessed: 17 September 2023).
[4] Shishkova, A.T. et al. (no date) Informe sobre las amenazas móviles en 2022, Securelist Spain. Available at: https://securelist.lat/mobile-threat-report-2022/97661/ (Accessed: 17 September 2023).
[5] ¿Qué es la ciberseguridad? (2023, August 17). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
[6] ¿Qué es el malware? (2020, July 10). McAfee. https://www.mcafee.com/es-co/antivirus/malware.html