inovtecshop®

FICHA TECNICA

Escaner de Malware y Spyware para dispositivos móviles Android e iOS - Detección forense con IA integrada

IN-0607D

ANÁLISIS

www.inovtecshop.com

Escáner de malware con IA para TSCM profesional e inteligencia contra amenazas móviles

Escanea, analiza, protege.

En las operaciones modernas de contravigilancia, los dispositivos móviles ya no son una preocupación secundaria; a menudo son la principal superficie de ataque. El smartphone se ha convertido en la plataforma de vigilancia más eficiente jamás creada: siempre encendido, siempre conectado, siempre cerca de su propietario.

El IN-0607D es un escáner profesional de malware impulsado por inteligencia artificial y una plataforma de inteligencia de amenazas móviles, diseñada para equipos de seguridad que no pueden permitirse puntos ciegos.

Desarrollado para especialistas en TSCM, directores de seguridad corporativa, fuerzas del orden, unidades militares y profesionales de inteligencia, el IN-0607D detecta malware, spyware de nivel gubernamental, comportamientos sospechosos y actividad de red encubierta tanto en dispositivos Android como iOS.

El IN-0607D es el hardware forense profesional más avanzado, diseñado para protección ejecutiva, detección de amenazas internas y spyware de nivel gubernamental.

No es una solución antivirus de consumo convencional.

Es un instrumento de detección forense listo para campo, **desarrollado para investigaciones reales** donde la integridad operativa, la confianza del cliente y la seguridad de la misión no son negociables.

El IN-0607D se destaca como un escáner profesional líder en detección de spyware móvil, ofreciendo identificación avanzada de amenazas ocultas en smartphones. Funciona eficazmente como un escáner forense de malware para iOS y Android, permitiendo análisis físico y de tráfico en profundidad para descubrir troyanos, spyware y anomalías que las herramientas convencionales suelen pasar por alto.

Además, el dispositivo opera como un escáner móvil confiable para TSCM, convirtiéndose en una herramienta esencial para profesionales de ciberseguridad, investigadores y organizaciones que realizan contramedidas técnicas de vigilancia en dispositivos móviles.

¿Por qué el escaneo de dispositivos móviles es crítico en las operaciones TSCM?

Las inspecciones tradicionales se centran en transmisores RF, cámaras ocultas y dispositivos físicos de escucha. Sin embargo, las herramientas de vigilancia más sofisticadas de hoy operan de forma silenciosa dentro de los smartphones. Cuando un dispositivo está comprometido, puede socavar toda una operación, exponer comunicaciones sensibles y generar una fuga de inteligencia oculta que ninguna inspección tradicional logrará detectar.

Para los profesionales encargados de la protección ejecutiva, la mitigación de amenazas internas, la defensa contra el espionaje corporativo o las operaciones clasificadas,

Los dispositivos móviles comprometidos pueden:

- Transmitir audio del micrófono de forma remota
- Exfiltrar documentos sensibles
- Rastrear el movimiento de ejecutivos en tiempo real
- Operar aplicaciones de vigilancia encubierta
- Ocultar comunicaciones de comando y control (C2)

El IN-0607D cierra esa brecha de vulnerabilidad al incorporar inteligencia móvil de nivel forense directamente en su flujo de trabajo TSCM.

Detección de malware y spyware basada en IA

En el núcleo del IN-0607D se encuentra un **motor de análisis conductual impulsado por inteligencia artificial** que utiliza tecnología avanzada de modelado de amenazas. En lugar de limitarse a comparar firmas conocidas, el sistema evalúa el comportamiento del dispositivo en su contexto, identificando anomalías, abuso de privilegios y patrones de alto riesgo que indican compromisos sofisticados.

Este enfoque es fundamental al enfrentarse a implantes personalizados, explotación de vulnerabilidades zero-day y herramientas de vigilancia de nivel gubernamental que están deliberadamente diseñadas para evadir las plataformas antivirus convencionales.

El sistema evalua:

- Aplicaciones instaladas
- Permisos activos del sistema (micrófono, cámara, ubicación, accesibilidad, administrador)
- Procesos en ejecución
- Modificaciones en archivos del sistema
- Patrones de comportamiento sospechosos
- Anomalías de red
- Posibles indicadores de spyware de nivel gubernamental

El resultado es una evaluación de amenazas clasificada por nivel de riesgo, con recomendaciones accionables que permiten a los equipos de seguridad pasar de la sospecha a hallazgos documentados con claridad y autoridad.

La operación de IA completamente offline garantiza la privacidad operativa durante intervenciones sensibles.

Escáner Android: análisis forense directo por USB

El módulo Android Scanner proporciona análisis del dispositivo **en tiempo real mediante conexión WebUSB**, permitiendo a los investigadores realizar exámenes controlados sin depender de servicios en la nube de terceros.

Diseñada para despliegue en campo, esta capacidad permite a los profesionales de TSCM y consultores forenses digitales realizar la evaluación inicial de dispositivos durante investigaciones activas, inspecciones de seguridad en viajes ejecutivos y operaciones corporativas de respuesta a incidentes.

Capacidades incluyen:

- Inspección completa de aplicaciones instaladas
- Análisis de permisos críticos (micrófono, cámara, GPS, accesibilidad, administrador)
- Evaluación de archivos del sistema
- Monitoreo de utilización de recursos
- Puntuación de riesgo mediante IA y clasificación de amenazas Generación profesional de informes en PDF

El proceso de escaneo es eficiente, lo que permite evaluaciones rápidas en sitio, manteniendo al mismo tiempo la capacidad de realizar análisis forenses más profundos cuando sea necesario.

Escáner iOS: análisis avanzado de Sysdiagnose

Los dispositivos Apple requieren un enfoque forense diferente. El IN-0607D aprovecha el análisis avanzado de archivos *sysdiagnose* para extraer inteligencia a partir de registros del sistema, datos de telemetría y líneas de tiempo de comportamiento.

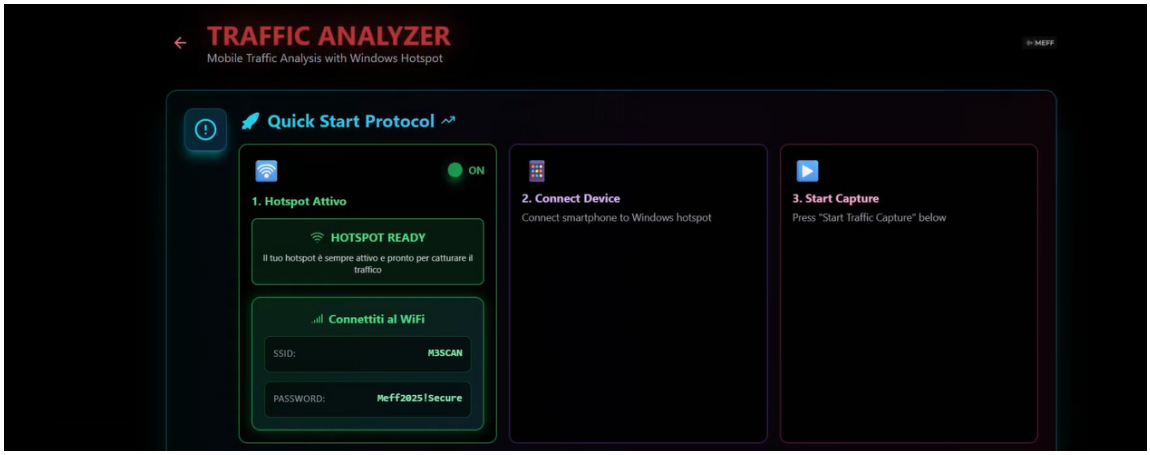
Esto proporciona a los investigadores una visibilidad estructurada sobre los patrones de comportamiento del dispositivo que, de otro modo, permanecerían ocultos dentro del sistema operativo.

La detección de amenazas en iOS incluye:

- Comportamiento sospechoso de aplicaciones
- Comunicaciones de red inusuales
- Indicadores conocidos de compromiso (IoC)
- Lista de verificación para detección de troyanos de nivel gubernamental
- Identificación de anomalías de comportamiento

Esto convierte al IN-0607D en una poderosa herramienta para auditorías de dispositivos ejecutivos, investigaciones sensibles a litigios y operaciones de seguridad en viajes de alto riesgo.

Analizador de Tráfico Integrado con Revisión de IA en Tiempo Real



La vigilancia no siempre reside dentro del dispositivo; con frecuencia se comunica hacia el exterior. La capacidad de observar el comportamiento a nivel de red transforma el escáner de una herramienta diagnóstica en una estación móvil de inteligencia de amenazas.

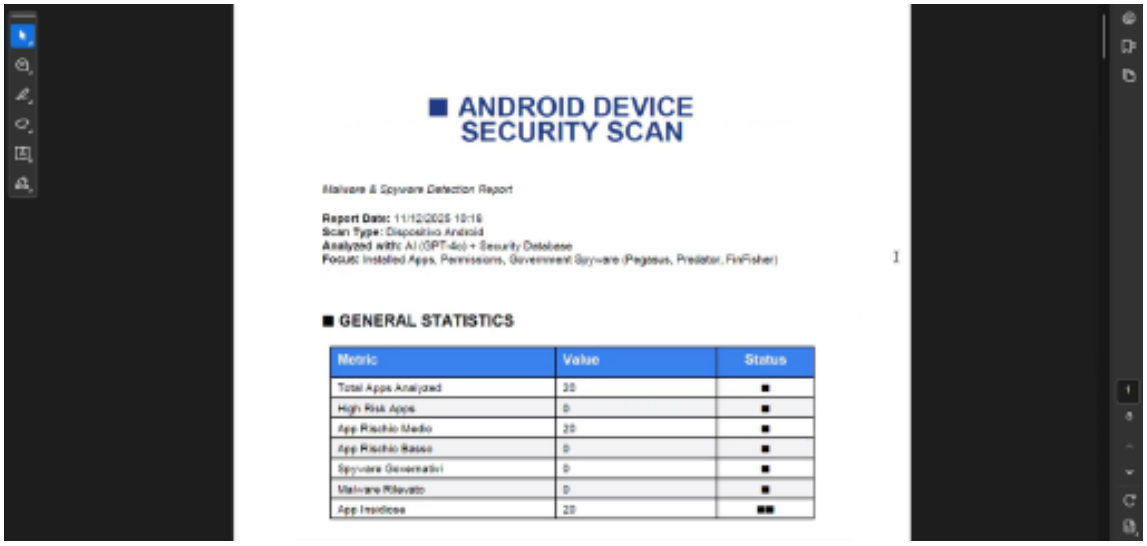
El módulo *Traffic Analyzer* captura e inspecciona tráfico de red a nivel de paquetes mediante modo monitor Wi-Fi o conexiones por cable tethering, permitiendo a los profesionales de seguridad observar patrones de comunicación en tiempo real.

Capturado y analizado:

- Comunicaciones HTTP / HTTPS
- Solicitudes DNS
- Tráfico saliente sospechoso
- Señales de comando y control (C2)
- Patrones encubiertos de exfiltración de datos

Después de la captura, el motor de IA evalúa el comportamiento del tráfico y resalta anomalías, dominios de interés y comunicaciones sospechosas, respaldando la toma de decisiones basada en evidencia durante operaciones activas.

Informes profesionales y documentación de pruebas



En entornos profesionales, los hallazgos deben estar documentados, ser defendibles y estar estructurados. El IN-0607D transforma análisis técnicos complejos en informes claros y exportables, adecuados para gobierno corporativo, procedimientos legales y revisiones internas de seguridad.

El IN-0607D genera:

- Informes PDF completos
- Exportaciones en formato JSON / CSV para flujos de trabajo forenses
- Líneas de tiempo de eventos
- Resúmenes de evidencia agrupada
- Orientación clara para la remediación

Los informes se organizan y almacenan de forma segura para su futura revisión.

Plataforma de hardware lista para el campo

Los entornos operativos exigen confiabilidad. Ya sea desplegado en una sala de juntas corporativa, una instalación gubernamental o una investigación remota en campo, el IN-0607D está diseñado para ofrecer durabilidad, facilidad de uso y desempeño profesional.

- Compacto y portátil
- Impulsado por batería
- USB-C para alimentación y transferencia de datos
- Interfaz táctil con tema oscuro
- Opción de línea de comandos (CLI) para flujos de trabajo forenses

Pasa sin problemas de las revisiones de la sala de juntas a las investigaciones de campo.

Protección de Datos y Seguridad Operativa

Al manejar dispositivos sensibles e investigaciones de alto riesgo, el propio escáner debe cumplir con estándares profesionales de seguridad. El IN-0607D protege la inteligencia recopilada mediante sólidas salvaguardas internas diseñadas para entornos de misión crítica.

El IN-0607D incluye:

- Almacenamiento cifrado con AES-256
- Acceso a claves protegido mediante frase de contraseña
- Eliminación segura de reportes temporales

Interfaz Multilingüe y Profesional

Diseñada para operaciones internacionales y uso multiagencia, la interfaz prioriza la claridad, el control y la gestión estructurada del flujo de trabajo.

- Soporte multilingüe (IT / EN / FR)
- Controles desde panel administrativo
- Sección organizada de reportes guardados

Sistema Opcional de Escaneo Remoto

Un sistema opcional de escaneo remoto para dispositivos iOS y Android amplía el alcance operativo, permitiendo escenarios de evaluación controlada cuando el acceso físico al dispositivo puede estar limitado.

Diseñado para y utilizado por:

El IN-0607D se integra perfectamente en operaciones de seguridad de alto nivel y flujos de trabajo profesionales de investigación.

- Equipos de Seguridad Corporativa
- Profesionales TSCM
- Agencias Federales
- Unidades de Inteligencia Militar
- Fuerzas de Tarea de Aplicación de la Ley
- Equipos de Protección Ejecutiva
- Consultores en Informática Forense

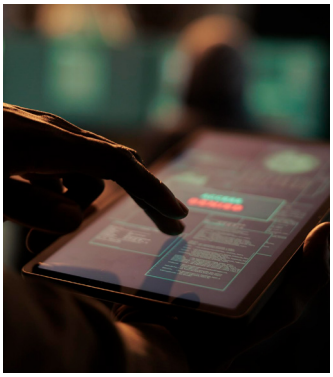
Casos de uso del escáner de malware móvil IN-0607D

Protección Ejecutiva

Permite a los equipos de seguridad corporativa y a los detalles de protección ejecutiva escanear rutinariamente teléfonos inteligentes de alto perfil en busca de spyware o troyanos avanzados que podrían permitir el seguimiento de la ubicación, la interceptación de llamadas o la exfiltración de datos, algo fundamental para proteger a los líderes de C-suite contra amenazas comerciales o patrocinadas por el estado.

Detección de Amenazas Internas

Ayuda a los centros de operaciones de seguridad (SOC) y a los investigadores empresariales a identificar dispositivos de empleados comprometidos que podrían estar filtrando datos corporativos confidenciales a servidores no autorizados, lo que ayuda a mitigar los riesgos de personas malintencionadas o vectores involuntarios explotados por actores externos.

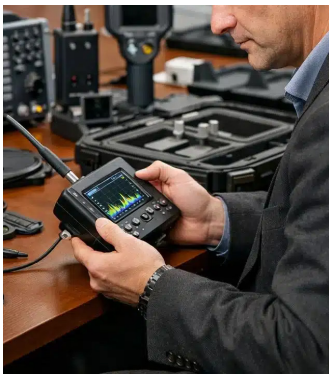


Detección de Spyware Gubernamental

Proporciona a las agencias gubernamentales, unidades militares y organizaciones de alta seguridad un análisis forense confiable para detectar software espía sofisticado de nivel gubernamental (por ejemplo, amenazas de clase Pegasus), utilizando escaneos físicos impulsados por IA, monitoreo de tráfico e informes certificados que cumplen con estándares internacionales como los de Amnistía Internacional.

Informática Forense e Investigaciones

Apoya a los equipos forenses e investigadores digitales en la realización de inspecciones exhaustivas de dispositivos para descubrir malware oculto, permisos sospechosos o comportamientos anómalos durante la respuesta a incidentes, casos legales u operaciones de contrainteligencia.



Contramedidas Técnicas de Vigilancia (TSCM)

Permite a los equipos de seguridad corporativa y a los detalles de protección ejecutiva escanear rutinariamente teléfonos inteligentes de alto perfil en busca de spyware o troyanos avanzados que podrían permitir el seguimiento de la ubicación, la interceptación de llamadas o la exfiltración de datos, algo fundamental para proteger a los líderes de C-suite contra amenazas comerciales o patrocinadas por el estado.

Seguridad Corporativa y Empresarial

Ideal para empresas sensibles a la seguridad que desean realizar una búsqueda proactiva de amenazas móviles, garantizando que los dispositivos utilizados por empleados en roles críticos permanezcan libres de software espía no detectado que las herramientas antivirus tradicionales a menudo pasan por alto.

IN-0607D vs Antivirus para consumidor

Los antivirus para consumidores convencionales reaccionan ante amenazas conocidas y bases de datos de firmas.

El IN-0607D analiza comportamiento, permisos, telemetría y tráfico de red a nivel profesional, ofreciendo información de grado investigativo en lugar de alertas superficiales.

Cuando un compromiso no es una simple molestia, sino una responsabilidad legal y operativa, se despliega detección de nivel profesional.

CONTACTO

Teléfonos
5557032846 y 6622070547

Correo
ventas@inovtec.com.mx

WhatsApp
5524229745

www.inovtecshop.com

Linktree

SIGUE NUESTROS ENLACES HACIENDO CLIC