smart info
CYBER SECURITY

Sistemi Anti Intercettazioni Telefoniche

Strumenti e sistemi a tutela della privacy anti-intercettazioni contro lo spionaggio industriale

Il Problema dello Spionaggio

Dati Allarmanti

Oltre l'87% delle perdite di dati avvengono con complicità interna. Le vittime sono intercettate nei colloqui riservati con infezione dello strumento informatico nel 50-60% dei casi e con malware dello smartphone nel 90% dei casi.

La cronaca ci racconta quanto accade dietro le spalle di soggetti potenti, sistematicamente "ascoltati" con totale violazione dei loro segreti, abitudini e privacy.

87%

Perdite Interne

Diffusioni di dati con complicità dall'interno

90%

Malware Mobile

Intercettazioni tramite smartphone infetti

Il Rischio dello Smartphone

Compagno di Vita

Affidabilità totale attribuita a uno strumento presente h24 per 365 giorni all'anno

Funzioni Multiple

Numerose app per uso professionale e ludico, senza conoscerne il reale funzionamento

Fattore Principale

Connettività, potenza di calcolo e storage lo rendono strumento di spionaggio a tuo sfavore

Le Soluzioni:

Proponiamo tre diverse soluzioni avanzate per prevenire efficacemente le intercettazioni telefoniche, garantendo la massima protezione della vostra privacy e delle informazioni sensibili.

Safety Box Anti Intercettazione

Dispositivo hardware che inibisce la possibilità di registrazione dei telefoni cellulari.

Mobile Threat Defence Software

Software di protezione in tempo reale contro malware e minacce per smartphone.

Spy Software Detection System

Sistema specializzato per identificarela presenza di software spia e trojan

Safety Box: Come Funziona

Il sistema innovativo genera un campo di disturbo acustico artificiale, impercettibile all'orecchio umano, che satura lo spettro delle frequenze audio. Questa "schermatura acustica" rende inefficace qualsiasi tentativo di intercettazione esterna, sia tramite microfoni ambientali nascosti che attraverso l'attivazione remota del microfono dello smartphone, bloccando di fatto attacchi di spionaggio basati su software o hardware. La tecnologia avanzata garantisce la protezione delle conversazioni più riservate in ambienti critici come sale riunioni, uffici direzionali, suite d'albergo, veicoli aziendali, aree riservate e durante incontri con partner strategici, clienti e colleghi. Questo assicura una tranquillità inestimabile, salvaguardando la proprietà intellettuale, i segreti commerciali e le strategie aziendali, fornendo massima riservatezza e integrità delle informazioni cruciali per il tuo business. Un'applicazione professionale indispensabile per la sicurezza delle tue comunicazioni sensibili.

01

Inserisci

Inserisci lo smartphone all'interno del cofanetto elegante in legno pregiato

02

Chiudi

Chiudi il cofanetto e attendi che si accenda la luce blu di sicurezza

03

Parla Liberamente

Nessuno potrà ascoltare attraverso l'hacking del cellulare. Privacy garantita!

Perché Altri Metodi Non Sono Sicuri

Smartphone Spento Non Basta

Se hackerato, l'admin nascosto può settare la registrazione audio-ambientale anche se spento, con invio dei file al riavvio. Alcune multinazionali hanno sistemi di ascolto permanente dell'utente.

Sacchetti Faraday Inefficaci

Disconnettono dalla rete ma non i microfoni. L'hacker può settare la registrazione prima dell'inserimento. Inoltre, perdi ricezione di chiamate, email e messaggi urgenti.

Funzioni di Ascolto Native

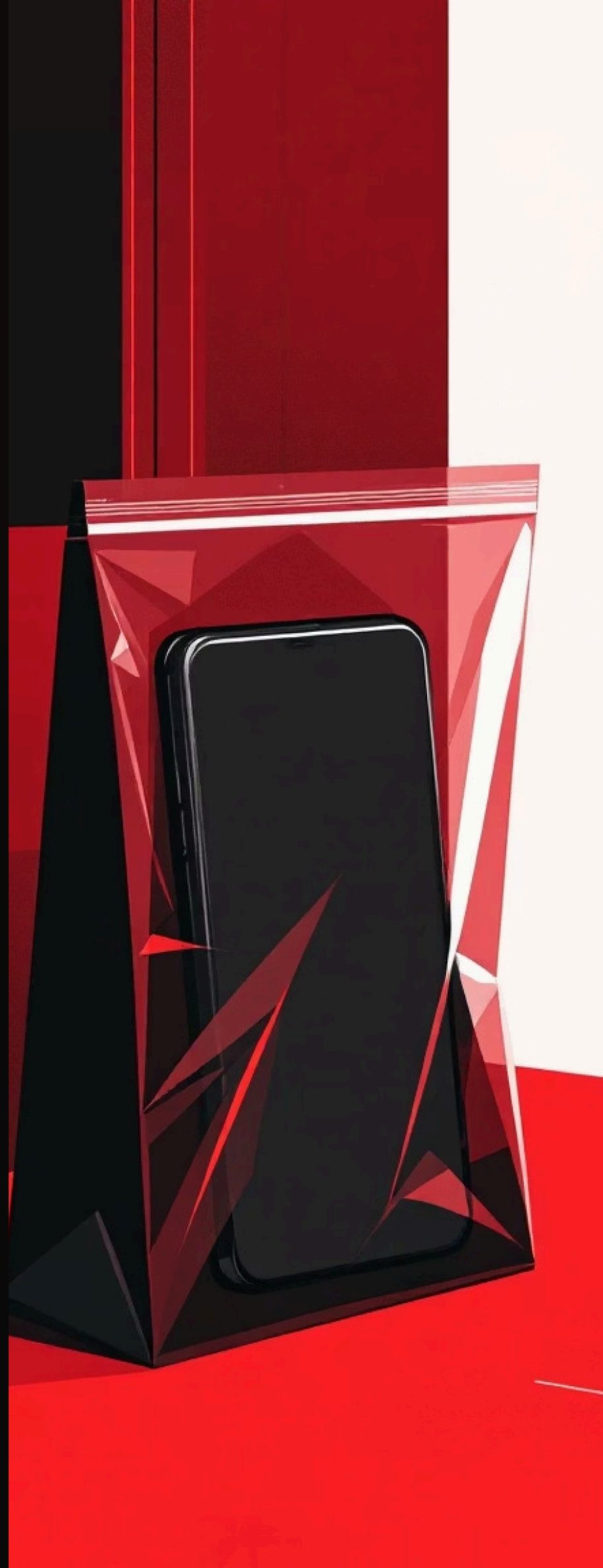
Gli smartphone Apple hanno "Ascolto dal Vivo" attraverso AirPods o Powerbeat. Il Sistema Anti Intercettazioni inibisce questa opportunità di ascolto ambientale.

Caratteristiche Premium

- Cofanetto elegante cm 13x22x5
- Sacca interna in velluto nero
- Personalizzazione disponibile

Autonomia Eccezionale

- Batteria fino a 20 giorni
- Ricarica veloce USB
- 2 ore = 96 ore consecutive



Modelli Disponibili

Modello S1

Ospita 1 telefono

Modello S2

Ospita fino a 2 telefoni

Modello S6

Ospita fino a 6 telefoni

Mobile Threat Defence Software

ERMETIX

Protezione di Nuova Generazione

Soluzione di sicurezza avanzata che protegge i dispositivi dalle minacce in tempo reale, salvaguardando dati e comunicazioni sensibili.

Architettura Unica

L'unica soluzione che integra nativamente UEM, EMM e MDM con un modulo MTD avanzato, offrendo un'architettura esclusiva sul mercato.

Compatibilità Universale

Piena compatibilità con ogni tipo di dispositivo: Android, Apple e Windows, garantendo una copertura completa e flessibile.

Gestione Unificata

Offre una gestione unificata e una protezione olistica contro ogni minaccia, semplificando la sicurezza mobile aziendale.

Mobile Threat Defence Software

Protezione in Tempo Reale

Identifica e blocca proattivamente malware, phishing, ransomware e minacce zero-day prima che possano compromettere il dispositivo o i dati.

Analisi Comportamentale Avanzata

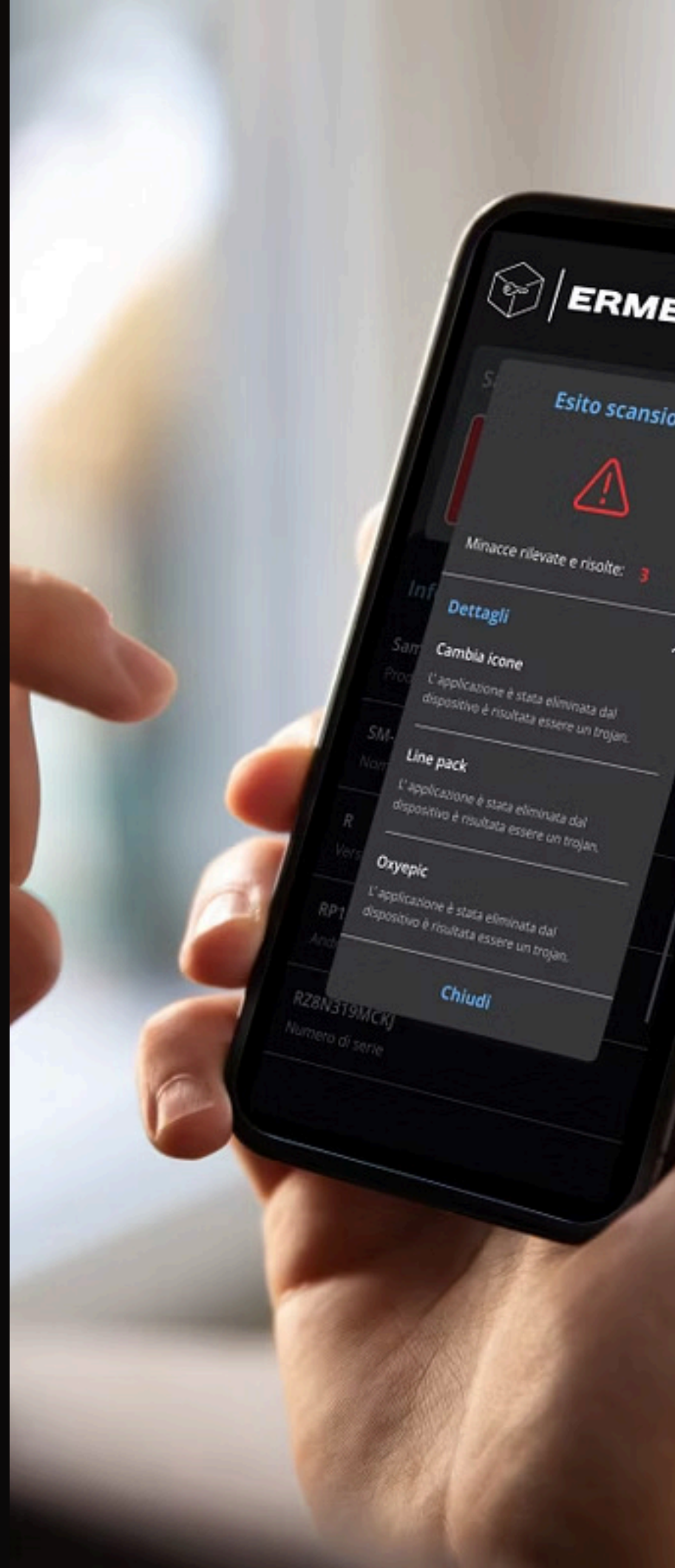
Monitora il comportamento di app e del sistema operativo per rilevare anomalie o attività sospette, segnalando potenziali compromissioni.

Sicurezza della Rete

Protegge da reti Wi-Fi non sicure, attacchi "man-in-the-middle" e connessioni dannose, garantendo comunicazioni cifrate e sicure.

Conformità e Gestione

Assicura il rispetto delle normative sulla protezione dei dati e offre strumenti centralizzati per la gestione della sicurezza su tutti i dispositivi aziendali.



Spy Software Detection System

Con questo apparato possiamo analizzare il traffico rete di qualsiasi Cellulare / Tablet o computer e comprendere se vi è un Trojan-Software Spy al suo interno. Il dispositivo utilizza la tecnologia di Sniffing – “Man in the Middle” passivo.

Rappresenta un salto qualitativo nel campo della cybersecurity, offrendo una soluzione all'avanguardia per la protezione contro le minacce digitali più sofisticate. Questo sistema intelligente è il risultato di un'approfondita analisi delle tattiche utilizzate dai cyber criminali nelle loro campagne contro istituzioni governative, imprese, organizzazioni della società civile e privati cittadini.

Il cuore dell'apparato è un motore di analisi avanzato che monitora costantemente il traffico di rete, alla ricerca di pattern sospetti. Il sistema si basa su un set di Indicatori di Compromissione accuratamente selezionati, che includono:

- **Anomalie nella gestione dei certificati di sicurezza**
- **Utilizzo improprio di servizi di certificazione gratuiti**
- **Impiego sospetto di infrastrutture DNS**
- **Comunicazioni su canali non convenzionali**
- **Attività legate a domini di recente creazione**
- **Trasmissioni non sicure o anomale**
- **Connessioni verso domini e/o IP potenzialmente malevoli**
- **Interazioni con reti anonimizzate**
- **Comunicazioni con reti note per attività illecite**

Grazie alla sua flessibilità algoritmica, alla versatilità di adattamento e alla capacità di analizzare comportamenti anomali e complessi, M2 Bridge New offre la possibilità di individuazione verso un'ampia gamma di minacce, dalle più comuni alle più sofisticate.

Caratteristiche Principali

Rappresenta una soluzione all'avanguardia per l'analisi forense e la rilevazione di spy software, garantendo massima efficacia e rispetto della privacy. La sua tecnologia innovativa offre un sistema di analisi rapido e autonomo, essenziale per la sicurezza delle comunicazioni sensibili.

NO TOUCH

Zero Contatto

Il dispositivo non viene mai toccato dall'operatore, preservando totalmente la privacy del cliente.

15-20 MIN

Analisi Rapida

Scansione completa in tempo record

REPORT

Certificato Legale

Viene elaborata una relazione completa dell'analisi con allegato un file .pcap per utilizzo forense.

Sicurezza e Autonomia

Funziona senza connessioni a server esterni o tunnel VPN, garantendo la totale autonomia del processo e aggiornamenti costanti.

Flessibilità e Portabilità

Compatibile con qualsiasi dispositivo e sistema operativo. Custodia antiurto con Wi-Fi, batteria a lunga durata e display iPad integrato.

Progettato per professionisti della sicurezza e investigatori, è uno strumento indispensabile per proteggere informazioni critiche in qualsiasi contesto operativo.