MOBILE SECURITY SCAN

ADVANCED MOBILE MALWARE & ZERO-DAY ANALYSIS

Government and Corporate Use
No Internet Connection Required

Fully offline
Government-grade
iOS & Android

OVERVIEW

MSS provides advanced analysis of mobile malware and zero-day threats by focusing on the fundamental mechanisms required for malicious operation. This approach enables reliable detection independent of malware obfuscation or evasion techniques. Designed for high-security environments, including government, defense, and enterprise.

CORE CONCEPT

All malware, regardless of sophistication, depends on two essential components:

- Entry Point – A method used to infiltrate the system (e.g., an infected file or malicious link).
- Exfiltration Channel – A communication pathway leveraged by malware to covertly transmit compromised data outside the system (e.g., HTTPS, DNS, email, or IP-based connections).

Even advanced malware - capable of hiding its presence and removing traces after installation - must establish an exfiltration channel to function.

MSS focuses precisely on monitoring these channels to detect and prevent data exfiltration.

TECHNICAL DETAIL

Supports Android & iOS
No root / jailbreak required
Kernel-level monitoring
YARA, IOC, AI-based analysis

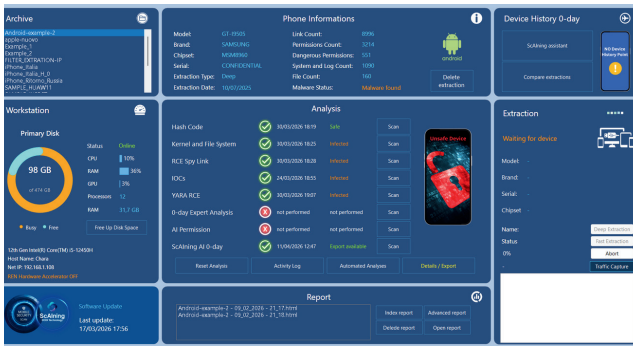
KEY CAPABILITIES

Zero-day protection
Fully offline operation
No signature dependency
Forensic-grade processes
Exfiltration monitoring
Data confidentiality

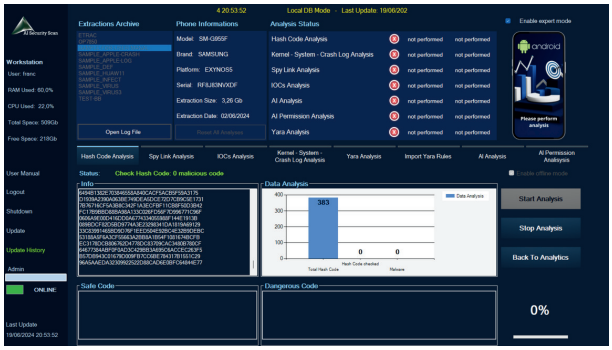
KEY HIGHLIGHTS

External Data & System Analysis
Secure data handling
Trusted by government & industry
Real-Time Traffic Monitoring
Privacy by Design
Deep System Analysis

Government



Corporate



Department Cyber Defense & Intelligence SA
Our Eyes Your Control

www.dcdi.io info@dcdi.io

Operations office: Via Livio 14, 6830 Chiasso, Switzerland
Registered office: Via alla Campagna 4, 6900 Lugano, Switzerland

MOBILE SECURITY SCAN

OPERATIONAL PROCESS

Extraction → Reverse Engineering → Identification → Analysis → Report

Phase 1: Extraction
Extracts system, configuration (e.g., crash logs, preload, certificates), diagnostic, and application files—excluding user data—without root, jailbreak, or agent installation.

Phase 2: Reverse Engineering
Core process used to extract and interpret hidden or non-readable application data (e.g., manifests, plist, XML, APK, IPA). This enables detection of advanced threats, including encrypted zero-days and modern RATs embedded within applications.

Phase 3: Identification and Collection
Post Reverse Engineering – Identifies and reconstructs spylinks, URLs, IPs, domains, ports, emails, phone numbers, tokens, and other configuration artifacts used in data exfiltration endpoints and channels.

Phase 4: Analysis
Users can perform individual analyses or enable automatic mode to run a full suite of scans, including **hash code, kernel & file system, spylink, IOC detection, YARA rules, AI permission analysis, and zero-day expert analysis.**

Phase 5: Report
Summarizes analysis results and detected threats, with optional user details and comments.

ADVANCED FUNCTIONS

Device History (Fast Differential Analysis):
Compares a trusted baseline extraction with a later extraction, such as before and after a trip, by analyzing hashes, app logs, and process logs, so malware analysis can focus only on detected changes and be completed in less time.

AI-Assisted Analysis (ScAIning):
AI assistant enabling automated threat analysis with interactive user support.

Traffic Monitoring:
Instead of relying on access points (e.g., routers or Wi-Fi) or tools such as Wireshark—which may miss advanced threats using encrypted or on-demand communication—MSS operates at the kernel level to monitor service ports and system activity.
This provides full visibility into processes, ports, and protocols, even when no packets are being actively transmitted.