APPLICATION AREAS:

ATTACKING CAPABILITIES

Along with gathering intelligence about the surrounding Wi-Fi landscape and proactively investigating network traffic to identify threats, Wi-Fi Hunter allows you to step even further. It features a built-in mechanism for selectively de-authenticating clients from their access points. This functionality works in harmony with existing mobile network monitoring setups and offers effortless Wi-Fi jamming for the selected client.

DIRECTIONAL FINDING

The advanced Wi-Fi Hunter features involve the ability to detect and locate nearby access points and Wi-Fi enabled devices with pinpoint accuracy.

COMPREHENSIVE THREAT DETECTION

Stay ahead of evolving attacks and vulnerabilities. Wi-Fi Hunter scans your environment and analyses all bypassing traffic to proactively detect any suspicious behavior. The functionality is beneficial to private clients who are willing to uncover threats in Wi-Fi networks, as well as governmental organizations that act against illegal usage of Wi-Fi monitoring systems. The detected attacks include KRACK attack, de-authentication attack, WPS brute-force attack and password brute-forcing for any access point.

ADVANCED INTELLIGENCE GATHERING

Wi-Fi Hunter supports a range of functionalities to gather intelligence about Wi-Fi networks in the encompassing area. Its capabilities include tracking active Wi-Fi clients, displaying a list of clients connected to each access point, capturing half and full handshakes, collecting probe requests and performing traffic recording, among many others.

USA SALES & DISTRIBUTION
COMSEC LLC
PHONE: 800-615-0392 EMAIL: LML@COMSECLLC.COM
Wi-Fi Hunter is an ultimate multi-purpose smartphone-based device that gives you complete transparency and control over surrounding Wi-Fi networks. From advanced threat detection algorithms in neighboring Wi-Fi networks to detailed data gathering, it is designed to reveal critical network information about your Wi-Fi landscape in an intuitive and informative way.

**Features Overview**

- Fully passive scanning of Wi-Fi channels in 2.4 GHz and 5 GHz.
- Collecting essential information about access points and stations — including probe requests, half and full handshakes.
- Identifying a list of clients connected to each access point.
- Directional finding technology, allowing to precisely locate any active signal-transmitting Wi-Fi device.
- Real-time detection of common attack types, such as KRACK, WPS brute-force, de-authentication, and basic brute-forcing attack.
- The built-in de-authentication mechanism, allowing to de-authenticate selected clients from Wi-Fi networks.
- Traffic recording in the.pcap file for the access point or station.
- Determining MAC address randomization.
- Disclosing hidden networks.

**Technical Characteristics**

| Frequency range                  | 2.4 GHz: Channels 1–14 (2402 MHz – 2494 MHz)  
|                                | 5 GHz: Channels 34–165 (5150 MHz – 5835 MHz) |
| Battery life                    | Up to 12 hours in scanning mode